# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>XenApp for UNIX</td>
<td>11</td>
</tr>
<tr>
<td>XenApp for UNIX</td>
<td>12</td>
</tr>
<tr>
<td>Citrix XenApp 4.0, with Feature Pack 2, for UNIX</td>
<td>13</td>
</tr>
<tr>
<td>XenApp 4.0, with Feature Pack 2, for UNIX Release Note</td>
<td>14</td>
</tr>
<tr>
<td>Citrix XenApp 4.0, with Feature Pack 2, for UNIX Readme</td>
<td>21</td>
</tr>
<tr>
<td>Licensing XenApp for UNIX</td>
<td>24</td>
</tr>
<tr>
<td>Citrix XenApp 4.0, with Feature Pack 1, for UNIX</td>
<td>28</td>
</tr>
<tr>
<td>Citrix XenApp 4.0, with Feature Pack 1, for UNIX Readme</td>
<td>29</td>
</tr>
<tr>
<td>XenApp for UNIX Administration</td>
<td>32</td>
</tr>
<tr>
<td>Introducing XenApp for UNIX</td>
<td>33</td>
</tr>
<tr>
<td>Key Features</td>
<td>34</td>
</tr>
<tr>
<td>What’s New in Feature Pack 1 for Version 4.0?</td>
<td>36</td>
</tr>
<tr>
<td>UNIX Command-Line Conventions</td>
<td>37</td>
</tr>
<tr>
<td>Getting Started Quickly</td>
<td>38</td>
</tr>
<tr>
<td>Deploying XenApp for UNIX</td>
<td>39</td>
</tr>
<tr>
<td>Before You Begin Installing</td>
<td>40</td>
</tr>
<tr>
<td>System Requirements</td>
<td>41</td>
</tr>
<tr>
<td>Hardware Requirements</td>
<td>42</td>
</tr>
<tr>
<td>Software Requirements</td>
<td>43</td>
</tr>
<tr>
<td>SSL Relay Requirements</td>
<td>45</td>
</tr>
<tr>
<td>Euro Currency Symbol Support</td>
<td>46</td>
</tr>
<tr>
<td>Installing XenApp</td>
<td>47</td>
</tr>
<tr>
<td>Creating the Administrator Users and Group</td>
<td>48</td>
</tr>
<tr>
<td>Installing XenApp Using the Installer Script</td>
<td>49</td>
</tr>
<tr>
<td>Performing an Unattended Install</td>
<td>52</td>
</tr>
<tr>
<td>Performing an Unattended Install on Solaris</td>
<td>53</td>
</tr>
<tr>
<td>Performing an Unattended Install on HP-UX</td>
<td>55</td>
</tr>
<tr>
<td>Performing an Unattended Install on AIX</td>
<td>56</td>
</tr>
<tr>
<td>After Unattended Installation</td>
<td>57</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Publishing an Application to Accept Parameters from the Plugin</td>
<td>106</td>
</tr>
<tr>
<td>Displaying Published Application Details</td>
<td>108</td>
</tr>
<tr>
<td>Maintaining Published Applications</td>
<td>110</td>
</tr>
<tr>
<td>Changing the Settings of a Published Application</td>
<td>111</td>
</tr>
<tr>
<td>Displaying and Changing the Icon File</td>
<td>114</td>
</tr>
<tr>
<td>Specifying Default Settings for Published Applications</td>
<td>116</td>
</tr>
<tr>
<td>Configuring User Access to Published Applications</td>
<td>118</td>
</tr>
<tr>
<td>Managing the Servers that Publish an Application</td>
<td>120</td>
</tr>
<tr>
<td>Deleting a Published Application from All Servers</td>
<td>122</td>
</tr>
<tr>
<td>Enabling and Disabling Published Applications</td>
<td>123</td>
</tr>
<tr>
<td>Creating a New Published Application from Existing Details</td>
<td>124</td>
</tr>
<tr>
<td>Renaming a Published Application</td>
<td>125</td>
</tr>
<tr>
<td>Restricting Connections to Published Applications Only</td>
<td>126</td>
</tr>
<tr>
<td>Configuring an Initial Program</td>
<td>127</td>
</tr>
<tr>
<td>Publishing Preconfigured Applications for Anonymous Use</td>
<td>128</td>
</tr>
<tr>
<td>Managing Servers, Users, and Sessions</td>
<td>131</td>
</tr>
<tr>
<td>Displaying Information about Users and Sessions</td>
<td>132</td>
</tr>
<tr>
<td>Displaying More Details or Details in a Different Format</td>
<td>134</td>
</tr>
<tr>
<td>About the Display</td>
<td>136</td>
</tr>
<tr>
<td>Displaying Information about Servers on the Network</td>
<td>137</td>
</tr>
<tr>
<td>Ending a Session</td>
<td>139</td>
</tr>
<tr>
<td>Logging off from a Session</td>
<td>140</td>
</tr>
<tr>
<td>Disconnecting a Session</td>
<td>141</td>
</tr>
<tr>
<td>Connecting to a Disconnected Session</td>
<td>142</td>
</tr>
<tr>
<td>Resetting a Session</td>
<td>143</td>
</tr>
<tr>
<td>Reconnecting to Load Balanced Sessions</td>
<td>144</td>
</tr>
<tr>
<td>Shadowing a User’s Session</td>
<td>145</td>
</tr>
<tr>
<td>Starting Shadowing</td>
<td>146</td>
</tr>
<tr>
<td>About Shadowing and the Clipboard</td>
<td>147</td>
</tr>
<tr>
<td>Ending Shadowing</td>
<td>148</td>
</tr>
<tr>
<td>Sending Messages to Users</td>
<td>149</td>
</tr>
<tr>
<td>Printing</td>
<td>151</td>
</tr>
<tr>
<td>Displaying Client Printers or Printer Ports</td>
<td>152</td>
</tr>
<tr>
<td>Printing from a Command Line</td>
<td>153</td>
</tr>
<tr>
<td>Printing from Applications</td>
<td>155</td>
</tr>
<tr>
<td>Troubleshooting Printing</td>
<td>156</td>
</tr>
<tr>
<td>Connecting to a Remote Server from an ICA Session</td>
<td>157</td>
</tr>
<tr>
<td>Configuration Topic</td>
<td>Page</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Configuring XenApp for UNIX</td>
<td>159</td>
</tr>
<tr>
<td>Configuring the Server</td>
<td>160</td>
</tr>
<tr>
<td>Controlling Logon Settings</td>
<td>161</td>
</tr>
<tr>
<td>Setting the Number of Permitted ICA Connections</td>
<td>164</td>
</tr>
<tr>
<td>Disabling New Logons</td>
<td>165</td>
</tr>
<tr>
<td>Controlling Behavior for Disconnected or Broken Connections</td>
<td>166</td>
</tr>
<tr>
<td>Enabling or Disabling Printing for Users</td>
<td>168</td>
</tr>
<tr>
<td>Enabling or Disabling Clipboard Mapping</td>
<td>169</td>
</tr>
<tr>
<td>Providing Additional Graphics Clipboard Support</td>
<td>170</td>
</tr>
<tr>
<td>Enabling or Disabling Shadowing</td>
<td>172</td>
</tr>
<tr>
<td>Controlling Time-Out Behavior</td>
<td>174</td>
</tr>
<tr>
<td>Allowing Users to Log on without a Home Directory</td>
<td>178</td>
</tr>
<tr>
<td>Configuring Mouse-Click Feedback for High Latency Connections</td>
<td>180</td>
</tr>
<tr>
<td>Generating and Using Server Configuration Details</td>
<td>183</td>
</tr>
<tr>
<td>Screensaver Setting Recommendations</td>
<td>185</td>
</tr>
<tr>
<td>Customizing the Appearance of XenApp</td>
<td>186</td>
</tr>
<tr>
<td>Customizing the Login Screen</td>
<td>187</td>
</tr>
<tr>
<td>Changing the Window Manager</td>
<td>188</td>
</tr>
<tr>
<td>Troubleshooting the ctxwm Window Manager</td>
<td>191</td>
</tr>
<tr>
<td>Changing the Font Path</td>
<td>193</td>
</tr>
<tr>
<td>Configuring X Server Settings</td>
<td>195</td>
</tr>
<tr>
<td>Configuring Backing Store</td>
<td>196</td>
</tr>
<tr>
<td>Interactive Performance Tuning</td>
<td>197</td>
</tr>
<tr>
<td>Configuration Required for Fixes to Take Effect</td>
<td>198</td>
</tr>
<tr>
<td>Fixing the Disappearing Text Cursor Problem</td>
<td>199</td>
</tr>
<tr>
<td>Enabling the Left-Hand Keypad of SPARC Keyboards</td>
<td>200</td>
</tr>
<tr>
<td>Fixing the Disappearing X Cursor Problem</td>
<td>201</td>
</tr>
<tr>
<td>Fixing Screen Refresh Problems</td>
<td>202</td>
</tr>
<tr>
<td>Fixing NUM LOCK Problems</td>
<td>203</td>
</tr>
<tr>
<td>Fixing Java Application Splash Screen Problems</td>
<td>204</td>
</tr>
<tr>
<td>Disabling Color Cursor Support</td>
<td>205</td>
</tr>
<tr>
<td>Disabling Scrollmouse Support</td>
<td>206</td>
</tr>
<tr>
<td>Color Depth Limitations</td>
<td>207</td>
</tr>
<tr>
<td>Multimonitor Display Limitations</td>
<td>208</td>
</tr>
<tr>
<td>Advanced Topics</td>
<td>209</td>
</tr>
<tr>
<td>Configuring Anonymous Users</td>
<td>210</td>
</tr>
<tr>
<td>Displaying Anonymous User Settings</td>
<td>211</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Configuring Anonymous User Settings</td>
<td>212</td>
</tr>
<tr>
<td>Changing the Number of Anonymous Users</td>
<td>213</td>
</tr>
<tr>
<td>Changing the Naming of Anonymous User Accounts</td>
<td>214</td>
</tr>
<tr>
<td>Setting an Idle Time-Out Period</td>
<td>215</td>
</tr>
<tr>
<td>Specifying a Particular Shell for Anonymous Users</td>
<td>216</td>
</tr>
<tr>
<td>Specifying User Ids for Anonymous Users</td>
<td>217</td>
</tr>
<tr>
<td>Troubleshooting Anonymous User Accounts</td>
<td>218</td>
</tr>
<tr>
<td>Configuring XenApp Security</td>
<td>219</td>
</tr>
<tr>
<td>Security Overview</td>
<td>220</td>
</tr>
<tr>
<td>Default Security Settings</td>
<td>223</td>
</tr>
<tr>
<td>Displaying Security Settings for a Function</td>
<td>224</td>
</tr>
<tr>
<td>Configuring Security Settings</td>
<td>225</td>
</tr>
<tr>
<td>To change a global security setting</td>
<td>226</td>
</tr>
<tr>
<td>To configure security for a user</td>
<td>227</td>
</tr>
<tr>
<td>To configure security for a group of users</td>
<td>228</td>
</tr>
<tr>
<td>To inherit a security setting</td>
<td>229</td>
</tr>
<tr>
<td>Examples</td>
<td>230</td>
</tr>
<tr>
<td>XenApp for UNIX and the ICA Browser Service</td>
<td>231</td>
</tr>
<tr>
<td>Controlling the Master Browser</td>
<td>232</td>
</tr>
<tr>
<td>Manipulating Master Browser Elections</td>
<td>233</td>
</tr>
<tr>
<td>Introducing a New Server</td>
<td>234</td>
</tr>
<tr>
<td>Biasing the Results of Elections</td>
<td>235</td>
</tr>
<tr>
<td>Configuring the ICA Browser</td>
<td>236</td>
</tr>
<tr>
<td>Starting and Stopping the ICA Browser</td>
<td>237</td>
</tr>
<tr>
<td>If a Server Uses Multiple Network Interface Cards</td>
<td>238</td>
</tr>
<tr>
<td>Load Balancing Published Applications</td>
<td>240</td>
</tr>
<tr>
<td>Load Balancing a Group of Servers</td>
<td>241</td>
</tr>
<tr>
<td>Tuning Load Balancing</td>
<td>242</td>
</tr>
<tr>
<td>Troubleshooting Load Balancing</td>
<td>245</td>
</tr>
<tr>
<td>Configuring ICA Gateways</td>
<td>246</td>
</tr>
<tr>
<td>Using ICA with Network Firewalls</td>
<td>247</td>
</tr>
<tr>
<td>ICA Browsing with Network Address Translation</td>
<td>248</td>
</tr>
<tr>
<td>Configuring the TCP/IP Port Number</td>
<td>249</td>
</tr>
<tr>
<td>Configuring Session Status Logging</td>
<td>251</td>
</tr>
<tr>
<td>Configuring the Operating System for a Large Number of Connections</td>
<td>252</td>
</tr>
<tr>
<td>Configuring a Solaris System</td>
<td>253</td>
</tr>
<tr>
<td>Changing the Number of Pseudo-Terminals</td>
<td>254</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Understanding the Threats to Secure Communications</td>
<td>357</td>
</tr>
<tr>
<td>Using SSL to Tackle Security Threats</td>
<td>359</td>
</tr>
<tr>
<td>Comparing SSL with Citrix SecureICA</td>
<td>360</td>
</tr>
<tr>
<td>About Cryptography</td>
<td>361</td>
</tr>
<tr>
<td>Getting Started - A Summary of the Steps</td>
<td>364</td>
</tr>
<tr>
<td>To get SSL Relay up and running</td>
<td>365</td>
</tr>
<tr>
<td>What to Do Next</td>
<td>366</td>
</tr>
<tr>
<td>Planning Your SSL Relay Deployment</td>
<td>367</td>
</tr>
<tr>
<td>Choosing an Appropriate Security Solution</td>
<td>368</td>
</tr>
<tr>
<td>Obtaining a Digital Certificate</td>
<td>369</td>
</tr>
<tr>
<td>Determining the Certificates Required</td>
<td>370</td>
</tr>
<tr>
<td>Using SSL with Load Balancing</td>
<td>375</td>
</tr>
<tr>
<td>Where Do I Get Certificates From?</td>
<td>376</td>
</tr>
<tr>
<td>Configuring ctxssl Access to Commands</td>
<td>378</td>
</tr>
<tr>
<td>Generating or Renewing a Certificate</td>
<td>379</td>
</tr>
<tr>
<td>To generate a CSR file</td>
<td>381</td>
</tr>
<tr>
<td>Sending a Certificate Signing Request file to a CA</td>
<td>382</td>
</tr>
<tr>
<td>Preparing for an Attack on Your Security</td>
<td>383</td>
</tr>
<tr>
<td>Planning the Renewal of Expired Certificates</td>
<td>384</td>
</tr>
<tr>
<td>What to Do Next</td>
<td>385</td>
</tr>
<tr>
<td>Installing Digital Certificates</td>
<td>386</td>
</tr>
<tr>
<td>Protecting the Private Key</td>
<td>387</td>
</tr>
<tr>
<td>Installing a Server Certificate on a Server</td>
<td>388</td>
</tr>
<tr>
<td>To install a server certificate requested using ctxcertreq</td>
<td>389</td>
</tr>
<tr>
<td>To install a server certificate not requested using ctxcertreq</td>
<td>391</td>
</tr>
<tr>
<td>Example - the CA emails the server certificate as one file</td>
<td>392</td>
</tr>
<tr>
<td>Example - the CA emails the server certificate as two files</td>
<td>393</td>
</tr>
<tr>
<td>Installing a Root Certificate</td>
<td>394</td>
</tr>
<tr>
<td>What to Do Next</td>
<td>395</td>
</tr>
<tr>
<td>Configuring SSL Relay</td>
<td>396</td>
</tr>
<tr>
<td>To enable or disable SSL Relay</td>
<td>397</td>
</tr>
<tr>
<td>Configuring SSL Relay Ready for Use</td>
<td>398</td>
</tr>
<tr>
<td>To configure SSL Relay ready for use</td>
<td>401</td>
</tr>
<tr>
<td>To start the SSL Relay</td>
<td>403</td>
</tr>
<tr>
<td>To stop the SSL Relay</td>
<td>404</td>
</tr>
<tr>
<td>Displaying a TCP Port’s Configuration</td>
<td>405</td>
</tr>
<tr>
<td>To display summary information for all the ports</td>
<td>406</td>
</tr>
</tbody>
</table>
XenApp for UNIX

- XenApp 4.0, with Feature Pack 1, for UNIX
- XenApp 4.0, with Feature Pack 2, for UNIX

Quick Links

- XenApp 4.0, with Feature Pack 1, for UNIX Readme
- XenApp 4.0, with Feature Pack 2, for UNIX Readme
XenApp for UNIX

- XenApp 4.0, with Feature Pack 1, for UNIX
- XenApp 4.0, with Feature Pack 2, for UNIX

Quick Links

- XenApp 4.0, with Feature Pack 1, for UNIX Readme
- XenApp 4.0, with Feature Pack 2, for UNIX Readme
Citrix XenApp 4.0, with Feature Pack 2, for UNIX

This section of eDocs contains up-to-date product information about installing, configuring, and administering XenApp 4.0, with Feature Pack 2, for UNIX.

Learn about the following important topics.

<table>
<thead>
<tr>
<th>XenApp 4.0, with Feature Pack 2, for UNIX Release Note</th>
<th>Summarizes the new features and enhancements and describes how to install or upgrade to this version. Use this release note in conjunction with your XenApp 4.0, with Feature Pack 1, for UNIX documentation.</th>
</tr>
</thead>
<tbody>
<tr>
<td>XenApp 4.0, with Feature Pack 2, for UNIX Readme</td>
<td>Known issues with this release of Citrix XenApp for UNIX</td>
</tr>
<tr>
<td>Third Party Attributions for XenApp 4.0, with Feature Pack 2, for UNIX</td>
<td>Compilation of third party licenses for software that may be delivered with XenApp for UNIX</td>
</tr>
<tr>
<td>Citrix License Server Readme, for Citrix XenApp 4.0, with Feature Pack 2, for UNIX</td>
<td>Installing, configuring and managing the Citrix License Server for UNIX</td>
</tr>
</tbody>
</table>
XenApp 4.0, with Feature Pack 2, for UNIX Release Note

This release note summarizes the new features and enhancements in XenApp 4.0, with Feature Pack 2, for UNIX and describes how to install or upgrade to this version.

Use this release note in conjunction with XenApp 4.0, with Feature Pack 1, for UNIX. All the information for Feature Pack 1 is valid for Feature Pack 2.

Known issues in this version are described in Citrix XenApp 4.0, with Feature Pack 2, for UNIX Readme.

What's New?

XenApp 4.0, with Feature Pack 2, for UNIX provides the following new features and enhancements, which are all described in more detail in subsequent sections of this release note:

- HDX Image Acceleration
- Pluggable/Loadable Authentication Modules (PAM/LAM) enhancements
- Advanced load balancing
- HP-UX 11i v3 support
- AIX 6.1 support
- X clients extension
- Group enumeration

XenApp for UNIX is no longer supported on Sun Solaris SPARC 8, IBM AIX POWER 5.1 and 5.2, and HP HP-UX PA-RISC 11.0. Special extended maintenance support is available for Sun Solaris SPARC 8: for further details please contact your Citrix representative.

Installing and Upgrading

If you are installing XenApp for UNIX for the first time, follow the installation instructions for installxau in XenApp 4.0, with Feature Pack 1, for UNIX.

Upgrading to XenApp 4.0, with Feature Pack 2, for UNIX from all previous versions is supported, and is described in the following sections.

Citrix recommends that you install this feature pack on all servers running XenApp 4.0 for UNIX.
The feature pack requires 15 MB of free space.

Upgrading on Solaris x86/x64

1. Download the file to a suitable directory on the server on which you want to install the feature pack.

2. Untar and uncompress the file by typing:

   `compress -dc PSE400SOLX061.tar.Z | tar xvf -`

3. Ensure there are no users logged on and stop the server, using the ctxshutdown command.

4. Log on as root.

5. In the directory containing the PSE400SOLX061 directory, install the feature pack by typing:

   `patchadd -M . PSE400SOLX061`

Upgrading on Solaris SPARC

1. Download the file to a suitable directory on the server on which you want to install the feature pack.

2. Untar and uncompress the file by typing:

   `compress -dc PSE400SOL061.tar.Z | tar xvf -`

3. Ensure there are no users logged on and stop the server, using the ctxshutdown command.

4. Log on as root.

5. In the directory containing the PSE400SOL061 directory, install the feature pack by typing:

   `patchadd -M . PSE400SOL061`
Upgrading on HP-UX

1. Download the file to a suitable directory on the server on which you want to install the feature pack.

2. Untar the file by typing:

   ```
tar -xvf PSE400HPUX061.tar
   
   This creates a file called PSE400HPUX061.depot.
   
   3. Ensure there are no users logged on and stop the server, using the ctxshutdown command.

   4. In the directory containing the file PSE400HPUX061.depot, install the hotfix by typing:

   ```
   swinstall -s `pwd`/PSE400HPUX061.depot PSE400HPUX061
   
   5. Log on as root.

   6. Once the installation is finished, check that the hotfix is among the list of Citrix products installed by typing:

   ```
   swlist | grep Citrix
Upgrading on AIX

1. Download the file to a suitable directory on the server on which you want to install the feature pack.

2. Untar the file, by typing:
   ```bash
   tar -x -v -f PSE400AIX061.tar
   ```
   This creates a file called Citrix.MetaFrame.4.0.0.61.bff.

3. Ensure there are no users logged on and stop the server, using the ctxshutdown command.

4. Log on as root.

5. Citrix recommends that you use SMIT to install the .bff file. If the installation fails, one reason may be that it was unable to produce the .toc file that it needs. To work around this, run the following command in the directory where you have placed the .bff file:
   ```bash
   inutoc `pwd`
   ```
   Run the smit command and select "Software Installation and maintenance", then "Install and Update Software", then "Install Software".

6. Input the path of the .bff file described in step 2. You will then be prompted by a series of flags you must set to Yes or No.
   All flags can be left at their default settings except “COMMIT software updates”, which has to be set to No to install the patch as a separate component so that it can be removed.

Making New Features Available

If you upgrade to Feature Pack 2, as opposed to running a fresh installation, then to make the new features available you must run the following command after completing the upgrade:

   ```bash
   ctxlsdcfg -m FeaturePack2
   ```

   This makes the features available on every server in the farm on which you have installed the feature pack.

HDX Image Acceleration

HDX Image Acceleration lets you find a balance between the quality of photographic image data as it appears on a user's device and the amount of bandwidth the images consume on their way from server to client.

Image Acceleration applies a lossy compression scheme to reduce the amount of image data that the server sends to the client for faster screen updates. The compression scheme
removes redundant or extraneous data from the images while attempting to minimize the perceptible loss of information. Under most circumstances, the data loss is barely visible and its effect nominal. However, Citrix recommends that you use discretion in applying this feature where preservation of image data may be vital, as in the case, for example, of X-ray images.

Lossy compression is enabled only when available throughput for a connection falls below the specified number of bytes per second. To specify the number, log on as an administrator, then at a command line type:

```
ctxcfg -k lossycomppthreshold=n
```

where \( n \) = any number from 0 to 104857600 (100 MB). The default value is 0, which means the feature is off.

To specify the compression quality, log on as an administrator, then at a command line type:

```
ctxcfg -k lossycomppquality=n
```

where \( n \) = any number from 20 to 95. The default value is 85. Choose high values for users who need to view images at a level near original quality. To achieve faster updates over slow links, choose lower values. The default value provides medium compression, giving good image quality and low bandwidth usage.

You must set the threshold and quality on each individual server in the farm.

For lossy compression to be used, this feature must also be supported and enabled on the client.

**PAM/LAM Enhancements**

Pluggable/Loadable Authentication Modules (PAM/LAM) allow you to select the authentication service you want to use, and plug-in and make available new authentication service modules without having to modify your applications. Solaris and HP-UX use PAM for user name and password validation. AIX has its own authentication framework, which is called the LAM system and provides similar functionality.

The integration of PAM and LAM with XenApp for UNIX’s authentication process has been enhanced as follows:

- User-specific PAM and LAM information messages can be displayed to the user in a popup dialog box. Examples include password expiry notices and messages informing the user that an account is locked. These messages are specific to the PAM and LAMs in use and are separate to XenApp for UNIX messages. By default, the messages are not displayed. To display the messages, log on to the relevant server as an administrator, then at a command line type:

  ```
  ctxcfg -k authdialogs=1
  ```

- A more extensive set of system administrator PAM and LAM error messages is now automatically gathered and logged to the system log file.
XenApp for UNIX sessions can be authenticated through two methods: direct, using the ctxlogin process, and indirect, using the XML service. The enhancements provided with this version are available only when you are using direct authentication.

### Advanced Load Balancing

You can build on the standard XenApp for UNIX load balancing capabilities based around the number of sessions on each server to take into account actual system load as reported by the 1, 5 and 15 minute run queue averages. These advanced capabilities can be used in isolation from the actual number of sessions or in conjunction with them to build up highly tuneable load balancing criteria.

You can base the way the server load is calculated on a number of parameter settings; you can control the effect of those settings on the server load by assigning a series of weightings to each parameter that establish its importance compared to the other parameters.

The ctxbal utility is provided to set and adjust the load balancing parameters in the following ways:

- Maximum number of user sessions allowed
- The weight to be applied to user sessions, 1 minute run queue averages, 5 minute run queue averages, and 15 run queue averages
- The bias value to be applied to the load
- Load factor

For more information on how to use advanced load balancing, including configuration and monitoring examples, see [http://support.citrix.com/article/ctx123584](http://support.citrix.com/article/ctx123584).

### HP-UX 11i v3 Support

XenApp 4.0, with Feature Pack 2, for UNIX supports HP-UX 11i v3 on HP PA-RISC.

If installation of XenApp for UNIX fails because of installation dependencies, retry installing with dependency checking suppressed. Citrix advises that you use this option only when there is no alternative solution.

To install XenApp for UNIX with dependency checking suppressed, use installxau with the `-d` option. This option is recognized only on HP-UX.


To verify whether your system has the correct ONC version installed, use this command:

```
/usr/sbin/swlist -l fileset | grep ONC
```

If the output looks like this:
NFS B.11.31.08 ONC/NFS; Network-File System, Information Services, Utilities

you have version 8 installed and CDM will work correctly.

AIX 6.1 Support

XenApp 4.0, with Feature Pack 2, for UNIX supports AIX 6.1 on IBM AIX POWER.

X Client Extension

You can configure the maximum number of clients an X server can accept. To specify the number of clients allowed, for each server, add -maxclients xxx to the XTW_OPTS line in the file ctxXtw.sh, where xxx is the maximum number of clients.

The default is 256. Any values lower than 256 are ignored. The maximum value is either 1024, or the maximum number of file descriptors the X server is allowed to have open, whichever is the lower. On most systems you will need to use the ulimit command to increase the soft limit for the number of open file descriptors allowed per process, to allow maxclients values of greater than 256 to take effect.

Group Enumeration

You can configure how groups files are processed by XenApp for UNIX servers by using the ctxcfg -k fullyenumerategroups=[0|1] parameter on each server.

By default, this is set to 1 and the server reads the entire groups database before processing user logons and other actions. If you do not want the server to read the entire groups database, set the value to 0.

In some cases, group authentication mechanisms such as NIS or LDAP do not always supply accurate information when processed by some standard OS facilities. This flag ensures accurate group processing is performed. Note that this can result in longer authentication times.
Citrix XenApp 4.0, with Feature Pack 2, for UNIX Readme

Readme Version: 1.0

This file contains the latest information relating to Citrix XenApp 4.0, with Feature Pack 2, for UNIX. Please read this file fully before using Citrix XenApp 4.0, with Feature Pack 2, for UNIX. It contains important information that may be more up to date than other documentation you have available.

Contents

- What's Included
- Finding Documentation
- Getting Support
- Usage Notes, Restrictions, and Known Issues

What's Included

XenApp 4.0, with Feature Pack 2, for UNIX includes:

- On the Solaris SPARC platform, a Solaris package in the solaris directory on the CD-ROM.
- On the Solaris x86/x64 platform, a Solaris package in the solaris_x86 directory on the CD-ROM.
- On the AIX platform, a SMIT installable package in the usr/sys/inst.images directory on the CD-ROM.
- On the HP-UX platform, a HP-UX Software Distributor Depot in the hpux directory on the CD-ROM.
- On all platforms, a Citrix XenApp for UNIX installation script called installxau in the top level directory on the CD-ROM.
- On all platforms, hotfix packages in the hotfixes directory on the CD-ROM.
- The Citrix License Server for UNIX in the ctxls directory on the CD-ROM.
Finding Documentation

To access complete and up-to-date product information, go to Citrix eDocs located at http://support.citrix.com/proddocs/index.jsp and expand the topics for your product.

After installing XenApp for UNIX, you can also view man pages for specific XenApp commands.

Getting Support

Citrix provides technical support primarily through Citrix Solutions Advisor. Contact your supplier for first-line support or use Citrix Online Technical Support to find the nearest Citrix Solutions Advisor.

Citrix offers online technical support services on the Citrix Support Web site. The Support page includes links to downloads, the Citrix Knowledge Center, Citrix Consulting Services, and other useful support pages.

Usage Notes, Restrictions, and Known Issues

Licensing Issues

To license Citrix XenApp 4.0, with Feature Pack 2, for UNIX, you require Enterprise or Platinum edition licenses.

If you are covered by Subscription Advantage dated 17th March 2010 or later, you can use your licenses for XenApp 4.0, with Feature Pack 2, for UNIX on Solaris SPARC, Solaris x86/x64, AIX POWER, or HP-UX PA-RISC.

The Citrix License Server for UNIX, which runs on Solaris 9, SPARC version, and Solaris 10, x86/x64 or SPARC versions, is available from the Citrix Web site. Choose Downloads > Citrix Licensing and select the License Server for UNIX.

To access licensing documentation in Citrix eDocs, go to Licensing Your Product at http://support.citrix.com/proddocs/topic/licensing/lic-library-node-wrapper.html.

Hotfix Packages

This release installs all hotfixes up to, and including, PSE400xxx061.

The hotfix packages, included on the CD-ROM, contain functional changes for the Feature Pack 2 release and are installed with the main product when using the installxau product installation script. Do not attempt to install the hotfix packages separately. All features included in these hotfix packages are described in the XenApp for UNIX documentation at http://support.citrix.com/proddocs/topic/xenapp/ps-unix-wrapper-all-versions.html.

Known Issues

Restart ctxload each time you change the ctxbal parameters. The ctxload utility is a tool that tracks and graphs the load balancing value over time. However, when ctxbal is used to change the way the load value is calculated, this is not automatically reflected in the ctxload graphical output. To address this issue, stop and restart ctxload. The load is then
logged correctly against the new ctxbal criteria.

Installation issues on HP-UX 11i. Dependency errors may prevent the installation of XenApp for UNIX on HP-UX 11i platforms. This problem occurs because of the way Java 1.4 and 1.5 are packaged on HP’s distribution DVDs. swinstall checks that any prerequisite or co-requisite software is complete, but on a PA system only the PA binaries and libraries are installed for Java; thus an error is generated. To address this issue, use the workaround involving the installxau -d option, as described in the XenApp 4.0, with Feature Pack 2, for UNIX Release Note. Alternatively, you can either install the IA versions of the binaries, which will increase disk usage, or download PA-only versions of these binaries from http://www.hp.com/go/java.

Installation issues on AIX. There is an issue with the AIX installer where installations on systems with only Java 6 installed may fail. To address this issue, install Java 5 or Java 1.4 before installing XenApp for UNIX. After installation of XenApp for UNIX is complete, you can remove the Java 5 or Java 1.4 distribution, leaving the Java 6 distribution intact.
Licensing XenApp for UNIX

Citrix License Server for UNIX provides licenses for Citrix XenApp 4.0 for UNIX and any feature packs released for this version.

The License Server for UNIX package includes:

- An install package, CTXSls. This is available on the XenApp for UNIX installation media, or you can download it from http://www.citrix.com/English/ss/downloads/details.asp?downloadId=1681208&productId=186&c1=pov1680320.

- Documentation: the FLEXnet License Administration Guide. The installed location for this guide is /opt/CTXSls/docs/FNP_11.5_LicenseAdministration.pdf.

For general information on Citrix Licensing, see Licensing Your Product. In this general set of topics, one of the main differences between the UNIX installation and the Windows installation is the file locations. The following table compares their locations:

<table>
<thead>
<tr>
<th>File</th>
<th>Location on Windows (32-bit)</th>
<th>Location on UNIX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor options file</td>
<td>C:\Program Files\Citrix\Licensing\MyFiles\CITRIX.opt</td>
<td>/etc/opt/CTXSls/CITRIX.opt</td>
</tr>
<tr>
<td>Citrix start-up license file</td>
<td>C:\Program Files\Citrix\Licensing\MyFiles\citrix_startup.lic</td>
<td>/etc/opt/CTXSls/citrix_startup.lic</td>
</tr>
<tr>
<td>License files</td>
<td>C:\Program Files\Citrix\Licensing\MyFiles*.lic</td>
<td>/etc/opt/CTXSls/<em>.</em>.lic</td>
</tr>
<tr>
<td>Citrix vendor daemon log file</td>
<td>C:\Program Files\Citrix\Licensing\LS\lmgrd_debug.log</td>
<td>/var/CTXSls/lmgrd_debug.log</td>
</tr>
</tbody>
</table>

**Hardware Requirements**

Requirements vary depending on the number of XenApp for UNIX servers using this license server. Any server capable of running XenApp for UNIX on the Solaris platform can run this license server.

For details about selecting a server, see the FLEXnet License Administration Guide.

**Software System Requirements**

The license server (32-bit only) is supported on:

- Solaris 9, SPARC version
- Solaris 10, x86/x64 or SPARC versions

Citrix recommends that you install the latest patches for the operating system that you are using. For information and downloads, see the Sun Microsystems, Inc. Web site.

**Installing the License Server**
1. Create the following groups and users. They can be either local accounts or remote accounts: for example, NIS, NIS+, or LDAP.

   - The lmadmin license server administrator group. Add the users that you want to become administrators to this group. This group is required by license server commands that demand special administration rights, but do not require root access to the UNIX system. The users in this group log on with their normal user accounts.

   - A ctxlsadm user. Add the user to the lmadmin group.

   Citrix recommends, for security reasons, that you disable logons for ctxlsadm user. If you do so, install licenses as root.

2. Log on as root on the server where you want to install the license server.

3. Change to the directory containing the package.

4. Run `/usr/sbin/pkgadd -d CTXSls`

5. At the prompt, type `all` (or press Enter to accept `all` as the default).

6. At the Do you want to install these as setuid/setgid files? prompt, type `y` to set the correct file permissions for the files and processes. Do not type `n`, because this causes the license server to operate incorrectly.

7. At the Do you want to continue with the installation of `<CTXSls>` prompt, type `y`. Do not type `n`, because this causes the license server to operate incorrectly.

   The installation continues until complete and a success message appears. An error message appears if the installation is not successful.

   Do not overwrite or remove the Citrix start-up license file, `/etc/opt/CTXSls/citrix_startup.lic`. This file is necessary for the license server to run correctly.

**Configuring the License Server**

You can configure the license server lmstart and lmstop scripts by editing the `/etc/opt/CTXSls/lm.conf` file, in which you will find an explanation of the options that are available.

**Uninstalling the License Server**

1. Log on as root on the server on which you installed the license server.

2. Stop the license server by typing `/opt/CTXSls/sbin/lmstop`.

3. Run `/usr/sbin/pkgrm CTXSls`.

4. At the Do you want to remove this package? prompt, type `y`.

5. At the Do you want to continue with the removal of this package prompt, type `y`. Do not type `n`, because the uninstall may fail. The uninstall continues until complete and a success message appears. An error message appears if the uninstall is not successful.
After you uninstall the license server, if you customized any configuration files and installed user licenses, remove the files from /etc/opt/CTXSls.

Obtaining your License Files

License files are downloaded and managed through the Citrix Activation System at http://www.mycitrix.com/. For information about obtaining your license files, see Licensing Your Product.

Installing your License Files

As either the root or the ctxlsadm user, copy the downloaded license files into the /etc/opt/CTXSls directory.

The ctxlsadm user and lmadmin group must have read access to the files. If the files were copied as root, run the following commands to set the permissions correctly:

```
chown ctxlsadm:lmadmin [license files]
chmod 640 [license files]
```

If a license file is copied into the /etc/opt/CTXSls directory after the license server is started, the license server needs to be stopped and restarted, or the /opt/CTXSls/sbin/lmreader -c [license file] command can be used to reread the license files. The option argument to the -c option can either be the /etc/opt/CTXSls directory, which will cause the rereading of all license files in that directory, or it can be an individual license file in that directory. Multiple -c options can be specified on the command line.

Starting the License Server

Any user in the lmadmin group, or root, can start the license server by running the /opt/CTXSls/sbin/lmstart command.

By default, a log file (/var/CTXSls/lmgrd_debug.log) is generated after the license server starts. This log file contains basic information about licenses in use. It also logs any rejected license requests.

Stopping the License Server

Any user in the lmadmin group, or root, can stop the license server by running the /opt/CTXSls/sbin/lmstop command.

Starting the License Server on a System Restart

The license server package automatically configures the system to restart the license server on system restart.

To disable this functionality, remove the hard-linked files:

```
/etc/rc2.d/K02CTXSls
/etc/rc2.d/S98CTXSls
```

To reenable this functionality, run the following commands:

```
ln /etc/init.d/CTXSls /etc/rc2.d/K02CTXSls
```
Viewing License Usage

You can view license usage by running the /opt/CTXSls/bin/lmstat command. In addition, add the -a option to display all checked out licenses.

For example:

```
bash-3.00$ lmstat -a
```

Flexible License Manager status on Tue 3/11/2008 17:10

License server status: 27000@sporty
License file(s) on sporty:
/etc/opt/CTXSls/MPS_MCM_ALL_EDITION_PROD.lic:/etc/opt/CTXSls/citrix_startup.lic:
sporty: license server UP (MASTER) v11.5

Vendor daemon status (on sporty):
CITRIX: UP v11.5

Feature usage info:
Users of MPS_PLT_CCU: (Total of 1000 licenses issued; Total of 0 licenses in use)
Users of MPS_ENT_CCU: (Total of 1000 licenses issued; Total of 0 licenses in use)
Users of MPS_STD_CCU: (Total of 1000 licenses issued; Total of 0 licenses in use)
Users of MPS_ADV_CCU: (Total of 1000 licenses issued; Total of 0 licenses in use)
Users of MCM_STD_CCU: (Total of 1000 licenses issued; Total of 0 licenses in use)
Users of CITRIX: (Total of 5000 licenses issued; Total of 0 licenses in use)

Backing Up Your Files

Back up the following files:

- /etc/opt/CTXSls/CITRIX.opt
- /etc/opt/CTXSls/lm.conf
- Any administrator-installed license files in /etc/opt/CTXSls
Citrix XenApp 4.0, with Feature Pack 1, for UNIX

This section of eDocs contains up-to-date product information about installing, configuring, and administering Citrix XenApp 4.0, with Feature Pack 1, for UNIX.

Learn about the following important topics.

<table>
<thead>
<tr>
<th><strong>Citrix XenApp 4.0, with Feature Pack 1, for UNIX Readme</strong></th>
<th>Known issues with this release of Citrix XenApp for UNIX</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Administration</strong></td>
<td>Install, configure and maintain Citrix XenApp for UNIX</td>
</tr>
<tr>
<td><strong>SSL Relay for UNIX Administration</strong></td>
<td>Plan, configure and maintain SSL Relay for XenApp for UNIX</td>
</tr>
<tr>
<td><strong>Third Party Attributions, for Citrix XenApp 4.0, with Feature Pack 1, for UNIX</strong></td>
<td>Compilation of third party licenses for software that may be delivered with XenApp for UNIX</td>
</tr>
<tr>
<td><strong>Citrix License Server Readme, for Citrix XenApp 4.0, with Feature Pack 1, for UNIX</strong></td>
<td>Installing, configuring and managing the Citrix License Server for UNIX</td>
</tr>
</tbody>
</table>
Citrix XenApp 4.0, with Feature Pack 1, for UNIX Readme

Readme Version: 1.0

This file contains the latest information relating to Citrix XenApp 4.0, with Feature Pack 1, for UNIX. Please read this file fully before using Citrix XenApp 4.0, with Feature Pack 1, for UNIX. It contains important information that may be more up to date than other documentation you have available.

Contents

- What's Included
- Finding Documentation
- Getting Support
- Usage Notes, Restrictions, and Known Issues

Whats Included

XenApp 4.0, with Feature Pack 1, for UNIX includes:

- On the Solaris SPARC platform, a Solaris package in the solaris directory on the CD-ROM.
- On the Solaris x86/x64 platform, a Solaris package in the solaris_x86 directory on the CD-ROM.
- On the AIX platform, a SMIT installable package in the sr/sys/inst.images directory on the CD-ROM.
- On the HP-UX platform, a HP-UX Software Distributor Depot in the hpux directory on the CD-ROM.
- On all platforms, a Citrix XenApp for UNIX installation script called installxau in the top level directory on the CD-ROM.
- On all platforms, hotfix packages in the hotfixes directory on the CD-ROM.
- The Citrix License Server for UNIX on the CD-ROM.
Finding Documentation

To access complete and up-to-date product information, go to Citrix eDocs located at http://support.citrix.com/proddocs/index.jsp and expand the topics for your product.

After installing XenApp for UNIX, you can also view man pages for specific XenApp commands.

Getting Support

Citrix provides technical support primarily through Citrix Solutions Advisor. Contact your supplier for first-line support or use Citrix Online Technical Support to find the nearest Citrix Solutions Advisor.

Citrix offers online technical support services on the Citrix Support Web site. The Support page includes links to downloads, the Citrix Knowledge Center, Citrix Consulting Services, and other useful support pages.

Usage Notes, Restrictions, and Known Issues

Licensing Issues

To license Citrix XenApp 4.0, with Feature Pack 1, for UNIX, you require Enterprise or Platinum edition licenses.

If you are covered by Subscription Advantage dated 27th April 2005 or later, you can use your licenses for Citrix Presentation Server for UNIX Version 4.0, Solaris SPARC, AIX, or HP-UX.

If you are covered by Subscription Advantage dated 22nd February 2007 or later, you can use your licenses for Citrix Presentation Server for UNIX Version 4.0 or later on any supported platform, including Solaris x86/x64.

The Citrix License Server for UNIX, which runs on Solaris 8, SPARC version, Solaris 9, SPARC version, and Solaris 10, x86/x64 or SPARC versions, is available from the Citrix Web site. Choose Downloads > Citrix Licensing and select the License Server for UNIX.

To access licensing documentation in Citrix eDocs, go to Licensing Your Product at http://support.citrix.com/proddocs/topic/licensing/lic-library-node-wrapper.html.

Hotfix Packages

This release installs all hotfixes up to, and including, PSE400xxx054.

The hotfix packages, included on the CD-ROM, contain functional changes for the Feature Pack 1 release and are installed with the main product when using the installxau product installation script. You should not attempt to install the hotfix packages separately. All features included in these hotfix packages are described in the XenApp for UNIX documentation at http://support.citrix.com/proddocs/topic/xenapp/ps-unix-wrapper-all-versions.html.

Known Issues
By default, XenApp for UNIX is now compatible with other Citrix license sharing mechanisms. However, changing the compatibility setting affects the way licenses are allocated by the license server. For this reason, Citrix recommends that you ensure all users are logged off, before running the ctxsldcfg -c command. For more information, see the XenApp for UNIX documentation at http://support.citrix.com/proddocs/topic/xenapp/ps-unix-wrapper-all-versions.html. [#195309]
XenApp for UNIX Administration

This section contains up-to-date product information about installing, configuring, and administering Citrix XenApp 4.0, with Feature Pack 1, for UNIX. These topics are for system administrators responsible for deploying and maintaining Citrix XenApp for UNIX.

<table>
<thead>
<tr>
<th>Introducing XenApp for UNIX</th>
<th>Configuring XenApp for UNIX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploying XenApp for UNIX</td>
<td>Advanced Topics</td>
</tr>
<tr>
<td>Introducing Server Farms</td>
<td>Using the Citrix XML Service</td>
</tr>
<tr>
<td>Licensing XenApp for UNIX</td>
<td>Using Client Drive Mapping</td>
</tr>
<tr>
<td>Publishing Applications and Desktops</td>
<td>Command Reference</td>
</tr>
<tr>
<td>Managing Servers, Users, and Sessions</td>
<td></td>
</tr>
</tbody>
</table>
Introducing XenApp for UNIX

Citrix XenApp for UNIX is a server-based software product that you can use to provide your users with uninterrupted, secure access to UNIX and Java applications.

You install XenApp on a UNIX computer that will be used as a server. Sun Solaris, HP-UX, and IBM AIX platforms are supported. XenApp allows multiple users to log on and run applications in separate, protected sessions on the same server. For example, you may want to make word processors, Web browsers, Java applications, a particular window manager, or custom applications available to users.

You install the plugin software on the client devices, so users can connect to the server from a client device, such as a Windows PC. The plugin software is provided free, and is available for a range of different devices. This allows users to connect to the server from various platforms.

XenApp uses the ICA protocol to send information between the client device and the server. The ICA protocol sends keystrokes, mouse clicks, and screen updates between the server and the client. The application processing remains on the server, which means that processing on the client is kept to a minimum. To the user of the client device, it appears as if the software is running locally on the client.

Because applications run on the server and not on the client device, users can connect from any client device. A Macintosh, a Windows PC, or another UNIX computer can be used; the application looks and feels the same on each client device.
Key Features

This topic describes the key features and benefits of using XenApp for UNIX.

**Rapid application deployment.** You can provide your users with access to UNIX and Java applications by publishing these applications using XenApp for UNIX. A published application is a predefined application or shell script and its associated environment. To access a published application, users connect to it using the software on the client device. The application runs in a separate, protected session on the server. When the user exits the application, the session closes.

**User access to UNIX desktops.** You can provide users with full access to the UNIX server desktop. Users can run any application available on the desktop, in any order, or simultaneously. The server desktop appears in a window on the client device.

**Integration with UNIX security and accounts.** XenApp uses the security setup on the UNIX server. Therefore, you do not need to set up new user accounts for XenApp. Users at the client device can log on using their existing UNIX user account and password. Solaris and HP-UX use Pluggable Authentication Modules (PAM) for user name and password validation; AIX uses its own authentication mechanism. Note that XenApp supplies the user name and password for authentication; if additional information is required for the authentication process, this is not supported. For more information about configuring PAM on Solaris and HP-UX computers, see the man page for “PAM.” For AIX, see the man page for “authenticate.”

**Special group and account for Citrix administrators.** XenApp requires you to create a special user group with the authority to run administration commands and start and stop the server. This is the administrator group, which is called ctxadm. The user ctxsrvr must be created and added to this group.

**Configurable permissions for access to features.** You can control which users or groups of users can use particular XenApp features, such as logging on, disconnecting, and sending messages to other sessions, using the XenApp security feature. See Configuring XenApp Security for further information.

**Guest user access.** XenApp includes special anonymous user accounts with limited permissions. You can use these accounts to provide users with guest access to published applications and a temporary working directory for use during the session.

**Shadowing user sessions.** You can display and interact (using your keyboard and mouse) with another user’s session from your own session. This feature is called shadowing. You can use shadowing to help remote users with training or technical support issues.

**Copying text and graphics between applications.** Users can copy text and graphics between server-based applications and applications running locally on the client device. The clipboard behaves as if all applications are running on the client device itself.

**Load balancing among servers.** You can publish the same application on a number of servers. Users connect to the published application and XenApp ensures that the connections are distributed among servers so that a particular server does not become overloaded. You can also tune the distribution of connections among a group of load
balanced servers.

**SSL security.** XenApp for UNIX includes support for SSL Relay, which allows you to secure communications using Version 3.0 of the Secure Sockets Layer (SSL) protocol. SSL provides server authentication, encryption of the data stream, and message integrity checks. You can use SSL Relay to secure communications between an SSL-enabled client device and a XenApp server, or in a Web Interface deployment, between the Web server and a XenApp server.

**Support for RSA SecurID.** Support for RSA SecurID Versions 4.2 and 5.0 is included, allowing your users to log on to XenApp computers using RSA SecurID authentication.

**XML Service and Web Interface deployment.** XenApp for UNIX includes support for the Citrix XML Service. The Citrix XML Service communicates information about the UNIX applications published in a server farm to the Web server component of the Web Interface deployment. The Citrix XML Service also provides users with HTTP (HyperText Transport Protocol) browsing.

**Support for server farms.** Server farm support provides powerful, enterprise-level management and administration capabilities by allowing you to group XenApp servers into server farms that can be managed as a single unit. This means you can easily configure features and settings for the entire farm, from a central location, rather than configuring each server individually. For example, you can publish the applications or resources you want to make available to users at the farm level, establishing configuration settings that pertain to all instances of the application running in the farm.
What’s New in Feature Pack 1 for Version 4.0?

Feature Pack 1 for Version 4.0 provides a number of new features and enhancements that together extend the capabilities and flexibility of XenApp for UNIX. These include:

**Message of the day facility.** This feature allows you to specify a message of the day to display to users as they log on. Text stored in `/var/CTXSmf/motd` appears in a message box before logon, up to a maximum size of 2 KB.

**Disable new logons.** This feature allows you to prevent any new logons to a particular server, though users can still reconnect to disconnected sessions. See Disabling New Logons to a Server for more information about configuring this feature.

**ICA stack enhancements.** These enhancements provide increased connection stability and greater stack throughput on heavily loaded servers.
UNIX Command-Line Conventions

Citrix XenApp for UNIX has a command-line interface, which means you type the commands to control the server at a command prompt. If you are not familiar with UNIX command lines, note that:

- All UNIX commands are case sensitive
- The spacing on the command line is important and must be followed exactly as described in the instructions

**Note:** Run only one instance of some XenApp for UNIX commands at any one time—these are the commands that cause configuration changes (rather than commands that just query and display information). If more than one instance runs simultaneously, you may get unpredictable results.
Getting Started Quickly

This topic provides an overview of the minimum steps required to install and set up a server running XenApp for UNIX. For full details of how to install XenApp, including step-by-step installation and configuration instructions, see Deploying XenApp for UNIX. Citrix recommends that you read this topic before installing XenApp for the first time.

1. Configure a Citrix License Server. Citrix recommends that you do this before you install XenApp for UNIX so that you can tell the installer script the details of the license server. If you set up a license server after installing XenApp, you will need to use the ctxlsdcfg command to configure communication with the license server manually. For more information about configuring a license server, see Licensing XenApp for UNIX and Getting Started with Citrix Licensing.

2. Consider the design of the server farm. For example, because the server that you create the farm on will become the Management Service Master (the server with authoritative control of the farm), ensure that you create the farm on an appropriate server. For more information about server farms, see Introducing Server Farms.

3. Set up the accounts for the administrator. Use the standard UNIX system tools to do this. Log on as root and create a group called ctxadm, and add the users that you want to become administrators to this group. You must also create a ctxsrvr user and add this to the ctxadm group. If you do not set up these accounts, the installer script can do this for you. For information about setting up the accounts, see Creating the Administrator Users and Group.

4. Install the XenApp software on your UNIX server. The easiest way to do this is by using the installer script, which guides you through each step and prompts you for the information that it requires. For information about installing XenApp, see Installing XenApp.

5. Start XenApp on the server using the command ctxsrv start all.

6. Install the plugin software on each client device you plan to use from the XenApp installation media, or from the Citrix Web site. For information about installing plugins, see the installation topic in the administrator’s guide for the plugin you plan to deploy.

7. After installing the plugin software, create ICA connections to your server and test that you can connect from each type of plugin. For information about creating a connection from a client device to a server, see the administrator’s guide for the appropriate plugin.

When you can connect to your server from a client device, your server is operational.

**Note:** There is an administrator’s guide for each plugin in the documentation directory on your XenApp installation media.
Deploying XenApp for UNIX

These topics describe how to install XenApp for UNIX and carry out initial tasks such as creating administrative users and groups, setting the paths to XenApp commands and man pages, and configuring event logging. They also provide details of how to remove XenApp.
Before You Begin Installing

Make sure that you read the following information before installing XenApp:

- **Licensing XenApp for UNIX.** If you intend to use the installer script, Citrix recommends that you set up the Citrix License Server before you install XenApp. If you do this before installing XenApp, the installer script configures communication with the license server for you. If you do it after, you need to use the ctxlsdcfg command to configure communication with the license server manually. For more information about setting up a license server, see *Getting Started with Citrix Licensing*.

- **Introducing Server Farms.** Consider the design of your server farm before installing XenApp. For example, because the server that you create the farm on will become the Management Service Master (the server with authoritative control of the farm), ensure that you create the farm on an appropriate server.

- **UNIX Operating System Requirements.** The UNIX Operating System must be installed before you install XenApp. You must also ensure that your operating system is configured to run XenApp, and that you install the required updates, as listed in this topic.

- **Creating the Administrator Users and Group.** Unless you intend to use the installer script to install XenApp, you must create the `ctxadm` group and the `ctxsrvr` and `ctxssl` users before you begin installation.

  **Note:** Make sure that all users who connect to the server have a home directory path that is valid on the server, and that can be written to by the user.

  If a user has no home directory and tries to connect, the logon fails. Note that you can configure the server to allow users whose home directories are unavailable to log on; for more information, see *Allowing Users to Log on without a Home Directory.*
System Requirements

These topics list the minimum hardware and software system requirements for XenApp for UNIX. They include information about required operating system patches, Java Runtime Environment requirements, SSL Relay requirements, and Euro-currency symbol support.
Hardware Requirements

The minimum computer specification depends upon how many connections are to be supported. As a general rule, Citrix recommends that each server has between 16 and 24 MB of RAM per ICA connection. However, you may need to increase this amount of RAM depending upon the type of applications your users are running and the session properties, such as color depth and size.

Note: On the Solaris SPARC platform, XenApp for UNIX is supported only on processors based on SPARC V8 architecture or later.
Software Requirements

Operating System Patches

Citrix recommends that you install the latest patches for the operating system you are using. For information and downloads, see your operating system manufacturer’s Web site.

On Solaris 8 SPARC, to prevent sessions from freezing when running XenApp, apply patch 108993-37 (or later). This patch is available from the Sun Microsystems Web site.

Java Runtime Environment Requirements

Citrix recommends that you install the latest patches for the Java runtime environment (JRE) you are using. For all platforms, ensure that the JRE installed on your system is Version 1.4.2. or higher. To obtain JRE versions, see the Web site for your operating system manufacturer.

On the Solaris platform, do not use the 64-bit Solaris JRE. XenApp for UNIX is compatible with the 32-bit Solaris JRE only.

On the AIX platform, XenApp for UNIX runs only with JRE Version 1.4.2 (any patch level).

On the HP-UX platform, you must use a JRE of 1.4.2.08 or lower when installing XenApp for UNIX. Using a JRE of 1.4.2.09 or later will result in a Java compatibility error when the ctxxmlmd daemon is started. After installation, you can apply a later JRE version and install the latest public hotfix that addresses this issue. The hotfix is available from the Citrix Web site: http://support.citrix.com/.

Note: Some platforms may require prerequisite patches for the JRE. See the Web site for your operating system manufacturer or contact your hardware vendor for details about the appropriate patches.

On the Solaris Platform

The Solaris edition of XenApp for UNIX requires one of the following:

- Solaris 8, SPARC version
- Solaris 9, SPARC version
- Solaris 10, x86/x64 or SPARC versions

Note: The Solaris x86/x64 edition of XenApp for UNIX is available only on Solaris 10.

The server must have an X Window system installed with the appropriate window manager for the platform; for example, CDE.
Software Requirements

The following operating system packages are required:

- SUNWxwoftX Window System optional fonts
- SUNWu8lconv modules for UTF-8 locale

Verify that these packages are installed using the pkginfo command.

Note: On Solaris 8, these two packages are installed when you do an end-user install.

The Iconv libraries must be installed; they are necessary for XenApp to run. Check that the following files exist in the /usr/lib/iconv folder:

UCS-2*.so UTF-8*.so 8859-1*.so

On the HP-UX Platform

The HP-UX edition of XenApp for UNIX requires:

- HP-UX Version 11
- HP-UX 11i

The server must have an X Window system installed with the appropriate window manager for the platform; for example, CDE.

Note: Due to an HP-UX system limitation, you cannot specify server names of more than eight characters when running XenApp for UNIX on the HP-UX operating system.

On the AIX Platform

The AIX edition of XenApp for UNIX requires AIX Versions 5.1, 5.2, or 5.3.

The server must have an X Window system installed with the appropriate window manager for the platform; for example, CDE.
SSL Relay Requirements

SSL Relay for UNIX is included automatically when you install XenApp for UNIX. SSL Relay provides server authentication, encryption of the data stream, and message integrity checks. The system requirements for SSL Relay are the same as for XenApp for UNIX. For more information, see the *Citrix XenApp SSL Relay for UNIX Administrator’s Guide*. 
Euro Currency Symbol Support

XenApp supports the ISO 8859-15 Euro-currency symbol, if the underlying UNIX operating system supports it. To ensure this support, you may need to install patches recommended by your operating system and hardware vendor. See the Web site for your operating system manufacturer or contact your hardware vendor for details about the appropriate patches and for instructions to ensure Euro symbol support.
Installing XenApp

You need to perform the following steps to install XenApp:

1. If you are installing XenApp for the first time, create the administrator user and group accounts. However, if you intend to use the installer script to install XenApp, the script creates these for you.

2. Install XenApp from the installation media.

3. If you are installing XenApp for the first time, add the XenApp path(s) to your path, so that you can run the commands.

4. Start the XenApp processes on the server.
Creating the Administrator Users and Group

Before you install XenApp, create the XenApp ctxadm administrator group and add the users that you want to become administrators to this group. The ctxadm group is required by some XenApp commands that demand special administration rights, but do not require root access to the UNIX system. The users in the ctxadm group log on with their normal user accounts. If you create a farm containing more than one server, the ctxadm group must be a network group visible to all servers in the farm.

You must also create a ctxsrvr user and add this to the ctxadm group. Citrix recommends that the ctxsrvr user not be a logon user account.

You must also create a ctxssl user and add this to the ctxadm group. This account is used for SSL Relay administration.

**Important:** Do not use the ctxadm group and ctxsrvr user account for any purposes other than XenApp system administration.

Do not use the ctxssl user account for any purposes other than SSL Relay administration.

The following procedure is different from the one Citrix recommended in previous versions of XenApp for UNIX. This new procedure is considered a security “best practice” because users in the ctxadm group log on with their normal user accounts and the ctxsrvr user is no longer a logon account.

**To create administrator group and user accounts**

1. Create the administrator’s group using the group name ctxadm.

2. Add the users that you want to become administrators to the ctxadm group.

3. Create a user account called ctxsrvr and add this user to the ctxadm group. Make sure the ctxsrvr user is not a logon user account (for example, set the shell for this user to be /etc/NoShell to prevent logons).

4. Create an SSL Relay administrator using the user name ctxssl. Make sure that you add the ctxssl user to the ctxadm group and that the ctxadm group is its primary group.
Installing XenApp Using the Installer Script

You can install XenApp for UNIX using the installer script provided. The installer script guides you through each step and prompts you for the information that it requires. This procedure works on all platforms.

**Note:** The following instructions describe a typical installation involving the creation of a new farm. You may see some or all of the following prompts, depending on the configuration of your system. For example, you see different prompts if you are joining a farm rather than creating a farm.
To install XenApp

1. Log on as root at the server on which you want to install XenApp.

2. Mount the XenApp installation media.

3. Change to the base directory of the XenApp installation media. For example, type: cd /cdrom The path is usually /cdrom/... but it may change depending on how your system mounts the installation media.

4. To start the package installer script and install XenApp, type: sh installxau [-b package_dir] [-p patch_dir] The install script has two options, -b and -p, which you can optionally use to customize your install process. By default, the install script looks for the install package on the installation media as follows:

   - $CDROOT/solaris/CTXSmf, for Solaris SPARC
   - $CDROOT/solaris_x86/CTXSmf, for Solaris x86/x64
   - $CDROOT/usr/sys/inst.images/Citrix.MetaFrame.bff, for AIX
   - $CDROOT/hpux/MetaFrame.depot, for HP-UX

   Using the -b option and supplying a location for package_dir, you can instruct the install script to look in the specified directory for the install package.

   Any hotfixes for the appropriate platform located on the CD-ROM in $CDROOT/hotfix will be installed automatically as part of the install, after the base install package has been installed and before the final configuration of the system takes place. These hotfixes are patch files that follow the Citrix patch file naming convention for this product: PSE4.0[SOL|SOLX|AIX|HPUX][0-9][0-9][0-9].tar[.Z]. These files do not require any uncompressing or unpacking to be used by the install script.

   Using the -p option and supplying a location for patch_dir, you can instruct the install script to look in the specified directory for hotfix patches to install. As XenApp for UNIX hotfixes contain all the changes from previous hotfixes, only the latest hotfix needs to be applied to fully patch an installation.

5. At the prompt for the license agreement, type y to accept the agreement and continue with installation. If you do not accept the license agreement, installation terminates.

6. At the prompt for server farm, type c (or create) to create a new server farm or j (or join) to join an existing farm.

7. If you are creating a new farm, at the prompt for the license server, type the name or network address of the license server.

8. If you are creating a new farm, at the prompt for the license server port number, type a port number or press ENTER to accept the default of 27000.

9. If you are creating a new farm, at the prompt for the product edition, type Enterprise or Platinum depending on which XenApp edition you are licensed to use, or press ENTER to accept the default of Enterprise.

   Note: If you do not know the details of the license server, you can configure the license server name, port, and product edition later using the ctxlsdcfg command.
10. At the prompt for the XML Service port number, type the port number the XML Service will use for connections to the Web Interface or press ENTER to accept the default of port 80. If port 80 is already in use, assign the XML Service to an unused port.

11. At the prompt for enabling SSL Relay, type y to enable SSL-secure connections to the server, or press ENTER to accept the default of n (not enabled). For more information about using SSL Relay, see the Citrix XenApp SSL Relay for UNIX Administrator’s Guide. If you are installing on an HP-UX or AIX platform, go to step 18.

12. At the prompt for the location of the Java Runtime Environment (JRE), type the path to the JRE; for example: /usr/j2re1.4.2_06.

13. At the prompt for the startup/shutdown script installation, type y if you want to start XenApp when the server is started and stop it when the server is shut down. If you answer yes, the script “S99ctxsrv” is installed in the /etc/rc2.d directory.

14. At the prompt for the man page installation, type y to install the XenApp man pages.

15. At the prompt for anonymous users, type y to create 15 anonymous user accounts, if you want to enable guest access.

   Note: When installing in a non-global zone on Solaris platforms, you are not given the option to enable anonymous user accounts. This is because by default XenApp creates the home directory for these users in the /usr filesystem, which is read-only in non-global zones. To enable anonymous users in such installations, run the ctxanoncfg -d utility to specify an alternative home directory after the main installation is complete. See Sun Microsystem’s Solaris Zones documentation to determine which file systems are read-only in a non-global zone.

16. At the prompt about security settings for setuid/setgid, type y to set the correct file permissions for the files and processes.

   Important: Do not type n, or XenApp will not operate correctly.

17. At the next prompt, type y to continue installing XenApp. When complete, a message tells you that the installation was successful.

18. At the prompt for farm name, type the name you want to give the farm.

19. At the prompt for farm passphrase, type a passphrase. Citrix recommends that you choose a suitably strong passphrase, in accordance with your company’s security policy.

   Note: You can use the ctxfarm command to change this passphrase later if necessary.

20. Confirm the passphrase.

   Installation is complete and you are now ready to start XenApp.

   Note: Do not attempt to share or copy the XenApp installation files between servers. The configuration database cannot be duplicated, and you will experience problems if you attempt to do this.
Performing an Unattended Install

These topics explain how to perform an unattended (quiet) installation on the various UNIX platforms. Unattended installation allows you to install XenApp quickly and easily on multiple servers, without prompting.
Performing an Unattended Install on Solaris

This topic explains how to perform an unattended installation on the Solaris platform. To do this, you use the administration and response files supplied on the XenApp installation media. You create a script file to run the unattended install using these files.

About the Response File

A response file, called response, is included in the /solaris or /solaris_x86 directory (as appropriate) on the XenApp installation media. This file is used by the -r option of the pkgadd command. This file includes the following:

- A basic XenApp for UNIX package is installed
- Fifteen anonymous users are added
- A startup script is installed
- man pages are installed

If you want to use different settings, copy and change this file as appropriate, or run pkgask to create a file of responses. For more information about pkgask, see its man page.

About the Administration File

An administration defaults file, called admin, is included in the /solaris or /solaris_x86 directory (as appropriate) on the XenApp installation media. This file is used by the -a option of the pkgadd command.

**Note:** The admin file assumes that the Java Runtime Environment is installed in /usr/j2se. If it is installed elsewhere, you must either edit a copy of the response file or make a symbolic link to the JRE.

The admin file permits running of install-time scripts as root, and installation of setuid/setgid binaries. It enforces dependency checking and disk-space checking.
To perform an unattended install on Solaris

1. Log on as root at the server on which you want to install XenApp.

2. Mount the XenApp installation media and locate the admin and response files in the Solaris directory.

3. Create a script file to perform the unattended install; for example:

   ```sh
   #!/bin/sh
   pkgadd -r /cdrom/solaris/response -a /cdrom/solaris/admin -d /cdrom/solaris/CTXSmf CTXSmf
   where /cdrom/solaris/admin is the administration defaults file, and /cdrom/solaris/response is the response file. The path is usually /cdrom/solaris/... but it may change depending on how your system mounts the installation media.

   Note: If you are installing on Solaris x86/x64, replace solaris in the above paths with solaris_x86.

4. Change permissions on the script file so that root can execute it; for example:

   ```sh
   chmod 744 scriptfile
   ```

5. Run the script file to start the unattended install.

6. When the unattended installation is complete, you must configure some settings manually. For more information, see After Unattended Installation.
Performing an Unattended Install on HP-UX

This topic explains how to perform an unattended install of XenApp on an HP-UX platform.

To perform an unattended install on HP-UX

1. Log on as root at the server on which you want to install XenApp.

2. Insert the XenApp installation media and mount it as a read-only filesystem. For example, at a command prompt type:

   ```
   mount -r /dev/dsk/c0t0d0 /mnt/cdrom
   ```

   where `/dev/dsk/c0t0d0` is the file that identifies the drive and `/mnt/cdrom` is the mount point of the installation media.

3. To install the entire XenApp package (including man pages, 15 anonymous user accounts, and the startup script), at the command prompt, type:

   ```
   swinstall -s /mnt/cdrom/ MetaFrame.depot MetaFrame
   ```

   Alternatively, list the particular filesets you want to install. For example, to install XenApp and the man pages, at a command prompt, type:

   ```
   swinstall -s /mnt/cdrom MetaFrame.Runtime MetaFrame.Man
   ```

   The following table describes the available filesets:

<table>
<thead>
<tr>
<th>Fileset</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anon</td>
<td>Choose to create 15 anonymous user accounts. You cannot install this fileset on its own—the Runtime fileset must also be installed.</td>
</tr>
<tr>
<td>Man</td>
<td>Choose to install the XenApp manual pages. You cannot install this fileset on its own—the Runtime fileset must also be installed.</td>
</tr>
<tr>
<td>Runtime</td>
<td>Choose to install the runtime environment (the programs and the configuration database).</td>
</tr>
<tr>
<td>Startup</td>
<td>Choose if you want to start XenApp when the computer is started and stop it when the machine is shut down. If you choose this fileset, the script ctxsrv is installed in the <code>/sbin/init.d</code> directory and two symbolic links are added:- The startup link <code>S999ctxsrv</code> is installed in <code>/sbin/rc3.d</code>- The shutdown link <code>K001ctxsrv</code> is installed in <code>/sbin/rc2.d</code>You cannot install this fileset on its own—the Runtime fileset must also be installed.</td>
</tr>
</tbody>
</table>

4. After the unattended installation is complete, you must configure some settings manually. For more information, see After Unattended Installation.
Performing an Unattended Install on AIX

This topic explains how to perform an unattended install of XenApp on an AIX platform.

**To perform an unattended install on AIX**

1. Log on as root at the server on which you want to install XenApp.

2. Insert the XenApp installation media.

3. To install the entire XenApp package (including man pages, 15 anonymous user accounts, and the startup script), at a command prompt, type:

   ```
   installp -X -d/dev/cd0 Citrix.MetaFrame
   ```

   where `-d/dev/cd0` is the installation media device, and `-X` ensures that there is sufficient disk space to install the package.

   Alternatively, list the particular filesets you want to install. For example, to install XenApp man pages, at a command prompt, type:

   ```
   installp -X -d/dev/cd0 Citrix.MetaFrame.man
   ```

   The following table describes the available filesets:

<table>
<thead>
<tr>
<th>Citrix.Metaframe...</th>
<th>Fileset description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.boot</td>
<td>Choose if you want to start XenApp when the computer is started and stop it when the computer is shut down. If you choose this fileset, the daemon ctxmfd is installed in /usr/lpp/CTXSmf/sbin and starts up automatically. During the installation of the .boot fileset, an entry is made in the /etc/inittab file that starts up ctxmfd and the server, when starting. You cannot install this fileset on its own—the Citrix.MetaFrame.rte fileset must also be installed.</td>
</tr>
<tr>
<td>.anon</td>
<td>Choose to create 15 anonymous user accounts. You cannot install this fileset on its own—the Citrix.MetaFrame.rte fileset must also be installed.</td>
</tr>
<tr>
<td>.rte</td>
<td>Choose to install the runtime environment (the programs and the configuration database).</td>
</tr>
<tr>
<td>.man</td>
<td>Choose to install the manual pages.</td>
</tr>
</tbody>
</table>

4. When the unattended installation is complete, you must configure some settings manually; for more information, see After Unattended Installation.
After performing an unattended installation, to complete the installation, you must configure the following settings manually:

- Set the XML Service port number using `ctxnfusesrv -port portnumber`
- Start the Management Service daemon using `ctxsrv start msd`
- Create or join a server farm using `ctxcreatefarm` or `ctxjoinfarm`
- Configure communication with the license server using `ctxlsdcfg`
- If you want to enable SSL Relay, write `SSL_ENABLED=1` to `/var/CTXSmf/ssl/config`
Setting the Paths to XenApp Commands

There are two types of XenApp commands:

<table>
<thead>
<tr>
<th>User commands</th>
<th>Any user can run these commands. They include the commands for logging off and disconnecting from a server. User commands are installed in the following directories:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>On HP-UX and Solaris:</td>
</tr>
<tr>
<td></td>
<td><code>/opt/CTXSmf/bin</code></td>
</tr>
<tr>
<td></td>
<td>On AIX:</td>
</tr>
<tr>
<td></td>
<td><code>/usr/lpp/CTXSmf/bin</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System administration commands</th>
<th>Only members of the <code>ctxadm</code> group can run these commands. They include server, published application, and ICA browser configuration tools. Administration commands are installed in the following directories:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>On HP-UX and Solaris:</td>
</tr>
<tr>
<td></td>
<td><code>/opt/CTXSmf/sbin</code></td>
</tr>
<tr>
<td></td>
<td>On AIX:</td>
</tr>
<tr>
<td></td>
<td><code>/usr/lpp/CTXSmf/sbin</code></td>
</tr>
</tbody>
</table>
Configuring User Access to Commands

Generally, you do not have to do anything to allow users to run user commands from their sessions. The path to these commands is added to each user’s path upon connection to the server, so any user can access XenApp user commands from an ICA session.

However, you may have to configure access to XenApp commands if the user’s shell script startup file (for example, .profile or .login) overrides the path. For example, on HP-UX, the default system profile (/etc/profile) sets the PATH environment variable explicitly.

To configure user access to XenApp commands

- If you are using a C shell, use a .login file for the user and add the path to the user commands. For example:

  On HP-UX and Solaris:

  ```bash
  setenv PATH ${PATH}:/opt/CTXSmf/bin
  ```

  On AIX:

  ```bash
  setenv PATH ${PATH}:/usr/lpp/CTXSmf/bin
  ```

- If you are using a Bourne or similar shell, use a .profile file for the user and add the path to the user commands. For example:

  On HP-UX and Solaris:

  ```bash
  PATH=${PATH}:/opt/CTXSmf/bin
  export PATH
  ```

  On AIX:

  ```bash
  PATH=${PATH}:/usr/lpp/CTXSmf/bin
  export PATH
  ```
Configuring Administrator Access to Commands

An administrator needs to be able to run both user and system administration commands. If you are installing XenApp for the first time, you need to configure your system so that administrators can run all the commands from the server console and also from an ICA session.

To configure administrator access to commands

- If you are using a C shell, use a .login file for the administrator and add the path to the user and administrator commands. For example:

  On HP-UX and Solaris:

  ```
  setenv PATH ${PATH}:/opt/CTXSmf/sbin:/opt/CTXSmf/bin
  ```

  On AIX:

  ```
  setenv PATH ${PATH}:/usr/lpp/CTXSmf/sbin:/usr/lpp/CTXSmf/bin
  ```

- If you are using a Bourne or similar shell use a .profile file for the administrator and add the path to the user and administrator commands. For example:

  On HP-UX and Solaris:

  ```
  PATH=${PATH}:/opt/CTXSmf/sbin:/opt/CTXSmf/bin
  export PATH
  ```

  On AIX:

  ```
  PATH=${PATH}:/usr/lpp/CTXSmf/sbin:/usr/lpp/CTXSmf/bin
  export PATH
  ```
Setting the Path to the man Pages

Generally, you do not have to do anything to allow users to display man pages for XenApp commands from a session. The path to these files is added to every user’s MANPATH environment variable upon connection to the server.

However, you may have to configure access to the man pages if the user’s shell script startup file (for example, .profile or .login) overrides the path. For example, on HP-UX, the default system profile (/etc/profile) sets the MANPATH environment variable explicitly.

To display the man pages from the server console when you log on as an administrator, you must set up your MANPATH environment variable to point to the location of the installed man pages. You need to do this only if you are installing XenApp for the first time.

To set the MANPATH environment variable

- If you are using a C shell:

  On HP-UX and Solaris:

  setenv MANPATH ${MANPATH}:/opt/CTXSmf/man

  On AIX:

  setenv MANPATH ${MANPATH}:/usr/lpp/CTXSmf/man

- If you are using a Bourne shell:

  On HP-UX and Solaris:

  MANPATH=${MANPATH}:/opt/CTXSmf/man
  export MANPATH

  On AIX:

  MANPATH=${MANPATH}:/usr/lpp/CTXSmf/man
  export MANPATH
Starting and Stopping XenApp

To start XenApp

When installation is complete, start the XenApp process on each server using the ctxsrv command.

**Note:** If, during installation, you choose to add the startup/shutdown script, XenApp automatically starts when the computer starts.

1. Log on to the server as an administrator.

2. At a command prompt, type:

```plaintext
ctxsrv start all
```

To stop XenApp

To stop the XenApp process on a server, use the ctxshutdown command. With ctxshutdown, you can specify when the shut down process will begin, and notify users that the server is about to shut down. This allows users to save their work and log off gracefully.

When the shut down process begins, applications will terminate, except for those that have registered window hints. These applications will attempt to interactively log users off by displaying a series of prompts.

With ctxshutdown, you can specify the maximum duration that users have to respond to these prompts. Any sessions that are still active when this period expires are terminated and the users are automatically logged off.

The server prevents users from logging on during the shut down process.

1. Log on to the server as an administrator.

2. At a command prompt:

<table>
<thead>
<tr>
<th>To</th>
<th>Use the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shut down the server using the defaults. By default, the server shutdown process begins after 60 seconds; the message “Server shutting down. Auto logoff in 60 seconds” is sent to all users logged on to the server. Applications that have registered window hints (the WM_DELETE_WINDOW attribute) have a further 30 seconds to interactively log users off before terminating.</td>
<td>ctxshutdown</td>
</tr>
<tr>
<td>Operate in quiet mode. This reduces the amount of information displayed to the administrator by the ctxshutdown command.</td>
<td>ctxshutdown -q</td>
</tr>
</tbody>
</table>
Specify when the shut down process will begin, and how long the message will appear, in seconds. The default is 60 seconds. When this period expires and the shut down process begins, applications that have registered window hints (the WM_DELETE_WINDOW attribute) will attempt to interactively log users off. Applications that have not registered window hints will terminate immediately.

```
ctxshutdown -m seconds
```

Specify how long applications that have registered window hints (the WM_DELETE_WINDOW attribute) have to interactively log users off. The default is 30 seconds. When this period expires, any remaining sessions are automatically terminated, users are automatically logged off, and the process stops.

```
ctxshutdown -l seconds
```

Specify the message displayed to all users logged on to the server. If you do not specify a message, the default message “Server shutting down. Auto logoff in x seconds” appears, where x = the number of seconds specified in the -m option (or the default of 60 seconds if this is not specified).

```
ctxshutdown message
```

**Example**

The following example shows how to display a message and begin the shut down process after two minutes. Applications that have registered window hints are given a further three minutes to attempt to interactively log users off.

```
ctxshutdown -m 120 -l 180 “Please log off now”
```
About Client Keyboard Support

XenApp supports client devices that use the following keyboards:

<table>
<thead>
<tr>
<th>Language</th>
<th>Locale ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>US English</td>
<td>409</td>
</tr>
<tr>
<td>UK English</td>
<td>809</td>
</tr>
<tr>
<td>French</td>
<td>40c</td>
</tr>
<tr>
<td>German</td>
<td>407</td>
</tr>
<tr>
<td>Swedish</td>
<td>41d</td>
</tr>
<tr>
<td>Spanish</td>
<td>40a</td>
</tr>
<tr>
<td>Italian</td>
<td>410</td>
</tr>
<tr>
<td>Danish</td>
<td>406</td>
</tr>
<tr>
<td>Dutch</td>
<td>413</td>
</tr>
<tr>
<td>Finnish</td>
<td>40b</td>
</tr>
<tr>
<td>Norwegian</td>
<td>414</td>
</tr>
<tr>
<td>Polish Programmers</td>
<td>415</td>
</tr>
<tr>
<td>Portuguese</td>
<td>816</td>
</tr>
<tr>
<td>Belgian Dutch</td>
<td>813</td>
</tr>
<tr>
<td>Korean (see note)</td>
<td>e0010412</td>
</tr>
<tr>
<td>French Canadian (see note)</td>
<td>c0c</td>
</tr>
<tr>
<td>Swiss German</td>
<td>807</td>
</tr>
<tr>
<td>Icelandic</td>
<td>40f</td>
</tr>
<tr>
<td>Japanese (see note)</td>
<td>e0010411</td>
</tr>
</tbody>
</table>

**Note:** The Korean and French Canadian keyboard locales are supported on the Citrix XenApp Plugin for Hosted Apps for Windows only. Only partial support for Japanese keyboards is available, allowing typing of English characters using a Japanese keyboard.
Configuring Non-English Keyboard Support

Your users can make connections to the server with client devices that use non-English keyboards. The keyboards that XenApp supports are shown in the table above.

To configure non-English keyboard support

1. Ensure you start the server in the country locale of the client keyboard that your users are employing. For example, if your users have German keyboards, start the server in a German locale. This ensures that the session runs in an appropriate locale where fonts containing the required keyboard symbols are in the font path and keyboard symbols appear correctly on the screen.

2. Make sure your users select the appropriate keyboard in the Settings dialog box on the client device. For further information about selecting keyboards, refer to the administrator’s guides for the plugins you are deploying.

Tip: You can alter the locale for an individual user by setting environment variables in the user’s start-up files.

Troubleshooting Non-English Keyboard Support

If users experience problems obtaining accent symbols, such as the circumflex accent (^), it may be that the application they are using does not support dead keys. A dead key is a key that does not produce a character when pressed—instead, it modifies the character produced by the next key press. For example, on a generic French PC keyboard, the circumflex (^) key is a dead key. When this key is pressed, and then the “a” key is pressed, “â” is generated.
Configuring Event Logging

When you first install XenApp, events are not configured to be sent to the system log (syslog).

XenApp uses the following event log levels:

- user.notice
- user.info
- user.warning
- user.err
- user.debug

To record XenApp events, add a line to the /etc/syslog.conf file and specify the event log levels that you want to record. You must be root to edit syslog.conf.

**Note:** The event log level names that XenApp uses may also be used by other programs. You may see messages from other software in the event log.

For example, adding the following line to the end of syslog.conf (separated with a tab, not a space) causes all event log messages from XenApp to be put in the file /var/adm/messages:

On Solaris and AIX:

```
user.notice;user.info /var/adm/messages
```

**Note:** The file that you use (that is, /var/adm/messages) must exist. If it does not, you must create it.

You may also want to send certain types of XenApp event details to the console. For example, to ensure that all error messages appear on the console, add this line to the file /etc/syslog.conf:

```
user.err /dev/console
```

**Note:** You can configure the logging of session logons, logoffs, disconnects, and reconnects using the ctxcfg command with the -k option.
For information, see Configuring Session Status Logging. For further details about configuring system event logging, see the syslog.conf man page.
Removing XenApp

Instructions for removing XenApp differ, depending on the operating system you are running. Procedures for removing XenApp from all supported operating systems are provided below.

To remove XenApp on Solaris

1. Log on to the server as an administrator.

2. Ensure that there are no active sessions and stop XenApp using the ctxshutdown command.

3. Log on as root.

4. To remove XenApp, type:

   pkgrm CTXSmf

To remove XenApp on HP-UX

1. Log on to the server as an administrator.

2. Ensure that there are no active sessions and stop XenApp using the ctxshutdown command.

3. Log on as root.

4. To remove XenApp, type:

   swremove

5. The SD Remove dialog box appears. Choose MetaFrame.

6. From the Actions menu, choose Mark for Remove.

7. From the Actions menu, choose Remove (analysis) to display analysis information prior to the installation. If any warnings are generated, display the Logfile for further details.


   Tip: To quickly remove the entire XenApp package, at a command prompt, type: swremove MetaFrame.
To remove XenApp on AIX

1. Log on to the server as an administrator

2. Ensure that there are no active sessions and stop XenApp using the ctxshutdown command.

3. Log on as root.

4. Type smit. The System Management Interface Tool dialog box appears.

5. Choose Software Installation and Maintenance.


7. Choose Remove Installed Software. The Remove Installed Software dialog box appears.

8. In SOFTWARE name, type Citrix.MetaFrame. To remove a particular fileset, type in its name; for example Citrix.MetaFrame.man.

   Note: If you want to remove the Citrix.MetaFrame.rte fileset, you must also remove the Citrix.MetaFrame.boot and Citrix.MetaFrame.anon filesets. If you do not, a “Dependency Failure” error message appears.

9. Set PREVIEW only? to no.

10. Choose OK.

11. At a prompt, choose OK to confirm you want to remove the software. When complete, check the Installation Summary to make sure that the removal was successful.

   Note: If the removal of XenApp fails, it may be because you did not stop the server—see Step 2.

12. To exit from smit, select Exit SMIT from the Exit menu.

   Tip: To quickly remove the entire XenApp package, at a command prompt, type: installp -u Citrix.MetaFrame.
What to Do Next

- If you set up the license server before installation and you used the installer script to install XenApp, your server is licensed and operational. If you did not set up the license server before installation or you did not configure communication with the license server during installation, set up the license server and use the ctxlsdcfg command to configure communication with it manually.

- If you did not configure the server farm during installation, you must create or join a server farm.

- Install the plugin software on each client device you plan to use from the XenApp installation media, or from the Citrix Web site. After installing the plugin software, create ICA connections to your server and test that you can connect from each type of plugin. For information about installing plugins and creating connections from a client device to a server, see the administrator's guide for the appropriate plugin.

When you can connect to your server from a client device, your server is operational.

- To provide your users with access to applications, publish applications using the ctxappcfg command.
Introducing Server Farms

A server farm is a group of XenApp servers that is managed as a single entity. Using a server farm allows you to:

- Deploy published applications and resources to all servers in the farm quickly and easily.

- Manage and administer settings for the entire farm from a single location, rather than configuring each server individually. You can administer the farm from any server in the farm; you do not need to connect remotely to other servers in the farm.

To create a server farm, you use the ctxcreatefarm command. After you create the farm, you use the ctxjoinfarm command to join other servers to the farm. The ctxcreatefarm and ctxjoinfarm commands are aliases of the ctxfarm command.

**Note:** If you are running this version of XenApp for UNIX alongside earlier versions in a server farm, ensure that the latest public hotfix is installed on all servers running earlier versions. You can download the latest hotfix from the Citrix Web site, at http://www.citrix.com.
Server Farm Components

The following diagram illustrates the key components in a typical server farm. The diagram shows the server where the administrator is logged on, the Management Service Master server, and other servers that are members of the farm. Secure communication between the various Management Services running on each server in the farm is also shown.

The Management Service Master

When you create a new server farm, the server on which you create the farm becomes the Management Service Master. The Management Service Master is a XenApp server that has authoritative control of the farm. The Management Service Master also holds the master copy of the farm’s data store.

Data Store

The data store is a human-readable text file that stores persistent data for the farm, such as configuration information about the servers and published applications in the farm. The Management Service Master holds the master file, while other servers in the farm each hold a copy of the data store.

When a server joins the farm, the data store is updated to reflect the addition of the new server, and the new server is given a copy of the farm’s data store.

The Management Service

The Management Service is a daemon that runs on each server in the farm that communicates server farm information, such as details about the published applications available in the farm.

When you make a configuration change to the server farm (for example, you publish a new application in the farm), the Management Service Master communicates this change to the
other servers in the farm using the Management Service.

Communication between the various Management Services in the farm takes place over a secure communication channel.

Secure Communication Channel

To protect sensitive information and administrator commands sent between servers, XenApp for UNIX provides a secure, private communication channel between all servers in a farm. This secure communication channel employs the Generic Security Service Application Program Interface (GSS-API) to provide mutual authentication of servers, and confidentiality and integrity protection for data transmitted across the network. GSS-API is an industry-standard security framework defined by the Internet Engineering Task Force RFC 2743. Authentication and data protection are performed by the Kerberos 5 GSS-API security mechanism (RFC 1964) in a way that avoids the need for an external Kerberos authentication server. Authentication instead depends on a shared secret that is securely distributed to servers when they join the server farm. The server farm passphrase is used for initial authentication when servers join the farm.

**Note:** You can use the ctxfarm command to change the farm passphrase and shared secret if necessary.

For secure communication between servers in a farm to function correctly, you must ensure that:

- **Clock settings on all servers in a farm are synchronized.** You can set up a network time server to ensure that clock settings on all servers in a farm are synchronized.

- **Name resolution between servers in a farm is consistent.** You should ensure that all servers to be placed in a farm resolve the names of other servers in the farm consistently. All servers must be able to resolve server names to IP addresses and IP addresses to server names.
Communication between Servers in a Farm

Interserver communication using the Secure Communication Channel occurs over TCP/IP on port number 2897. This communication consists of administration commands and management information updates and queries.

Interserver communication between ICA browsers occurs over UDP on port number 1604. This communication consists of UDP broadcasts to locate or elect the master browser for the local network or subnet, and UDP packets directed to the master browser to send server information updates and queries. The master browser holds information about each server’s address, load, available applications, and disconnected sessions.
Multiple Farms and Subnet Considerations

Citrix recommends that all servers in a farm are on one subnet. If servers in a farm are on different subnets, you must configure an ICA gateway to allow the servers to contact one another.

If you must create multiple farms on one subnet, ensure that published applications have different names in the different farms. For example, name the Diary application “DiaryA” in server farm A, and “DiaryB” in server farm B. This ensures that the Diary application is not load balanced over the two different farms and that users get consistent results, regardless of how they browse for applications.

**Note:** For more information about configuring ICA gateways, see Configuring ICA Gateways.
Integrating with Other XenApp Servers

Cross-server administration between Windows and UNIX versions of XenApp is not possible. Only servers running XenApp for UNIX can become part of a UNIX server farm. Similarly, only servers running XenApp for Windows can become part of a Windows server farm.

XenApp for UNIX will coexist with other servers running XenApp (for example, XenApp for Windows) on a network by sharing master browser information.

You can make applications published on XenApp for UNIX servers appear in the same location as applications published on XenApp for Windows farms. To do this, you use the Citrix XML Service with the multiple server farm functionality in the Web Interface. The Citrix Web Interface is an application portal technology that lets you integrate and publish applications to a Web browser from any standard Web server. For more information, see the Web Interface Administrator’s Guide. The Citrix XML Service is included automatically when you install XenApp for UNIX.
Creating a Server Farm

When you install XenApp for UNIX using the installer script, you are prompted to create a server farm or join an existing farm during the installation process. These topics describe how to create or join server farms manually using the ctxcreatefarm and ctxjoinfarm commands.

To create a server farm, you use the ctxcreatefarm command. Because the server that you create the farm on will become the Management Service Master, ensure that you create the farm on an appropriate computer.

When you create a farm, you are prompted for a passphrase. Citrix recommends that you choose a suitably strong passphrase, in accordance with your company’s security policy. You can use the ctxfarm command to change the farm passphrase later if necessary.

**Note:** You must remember this passphrase, because the passphrase you specify when you create the farm will be required by administrators whenever they attempt to join servers to this farm. If you lose the passphrase, you cannot add servers to the farm.

**To create a server farm**

1. Log on to the server that will become the Management Service Master as an administrator.

2. At a command prompt, type:

   ctxcreatefarm

3. At the prompt for farm name, type the name you want to give the farm.

4. At the prompt for passphrase, type a passphrase.

5. Confirm the passphrase.
Joining a Server Farm

After creating a server farm, you can join other servers to the farm using the ctxjoinfarm command. For security, before you can join a server to a farm, you need to know the passphrase specified for the farm. When you join a server to a farm, the server is updated with a copy of the new farm’s configuration.

To join a server farm

1. Log on to the server that you want to join to the farm as an administrator.
2. At a command prompt, type:
   
   ctxjoinfarm
3. At the prompt for farm name, type the name of the farm you want the server to join.
4. At the prompt for passphrase, type the passphrase specified for the farm.
5. At the prompt for server name, type the name or IP address of a server already in this farm.

XenApp communicates with the server farm and automatically joins the server to the farm.
Moving a Server to a Different Farm

You can use the ctxjoinfarm command to move a server to a different farm.

When you move a server to a different farm, the data store in the old farm is updated to reflect the removal of the server, and the server is updated with a copy of the new farm’s configuration. However, any published applications that were on the server in the old farm are no longer available in the new farm. To make these applications available in the new farm, you must publish them using ctxappcfg publish.

To move a server to a different farm

1. Log on to the server that you want to move to a different farm as an administrator.

2. At a command prompt, type:
   
   ctxjoinfarm

3. At the prompt for farm name, type the name of the farm you want the server to join.

4. At the prompt for passphrase, type the passphrase specified for the farm.

5. At the prompt for server name, type the name or IP address of a server already in this farm.

6. At the prompt, confirm that you want to move the server to the new farm. XenApp communicates with the server farm and automatically joins the server to the farm.
Troubleshooting Joining a Server Farm

Note: On HP-UX, due to an operating system limitation, you cannot specify server names of more than eight characters when running XenApp for UNIX.

If you experience problems attempting to join a server to a farm, check that:

- **Clock settings on all servers are synchronized.** You can set up a network time server to ensure that clock settings on servers already in a farm and servers joining the farm are synchronized. New servers cannot join the farm if clock settings are not synchronized.

- **Name resolution between servers is consistent.** You should ensure that all servers in a farm resolve the names of servers joining the farm consistently. If name resolution is not consistent, new servers cannot join a farm.

- **All servers are running the latest public hotfix.** If joining a server running this version of XenApp for UNIX to a farm created using a previous version fails, ensure that all the servers in the farm are running the latest public hotfix. On the Management Service Master, run the ctxfarm -k command to change the farm passphrase, and then retry joining the server to the farm.
Removing a Server from a Farm

You can remove a server from a farm using the ctxfarm -r command.

**Note:** You cannot remove the Management Service Master from a farm. Only members of a server farm that are not the Management Service Master can be removed from a farm.

When a server is removed from a farm, its copy of the farm data store is removed and published applications are no longer available from this server.

A server can be removed from a farm even when this server is unavailable. To do this, you log onto another server in the farm and remove the server. The remaining servers in the farm delete the information they hold about the removed server. You can also remove a server from a farm even when the Management Service Master is unavailable (for example, if the Management Service Master goes down).

**To remove a server from the farm**

1. Log on to a server in the farm as an administrator.

2. At a command prompt, type:

   ```
   ctxfarm -r [server-name]
   ```

   where **server-name** is the name of the server you want to remove from the farm. If you do not specify a server name, the local server is removed from the farm.
Renaming a Server

You cannot rename a server using the ctxfarm command.

To rename a server you must remove the server from the farm using the ctxfarm -r command. Note that you cannot remove the Management Service Master from a farm. Also, when you remove a server, any published applications available on this server are deleted.

Rename the server, then add the server to the farm again using the ctxjoinfarm command.
Identifying Servers in a Farm

You can identify the servers in a farm using the ctxfarm -l command. The list provides details of all the servers currently in a farm and also identifies the Management Service Master.

To identify the servers in a farm

1. Log on to a server in the farm as an administrator.

2. At a command prompt, type:

   ctxfarm -l
What to Do Next

After creating a server farm and joining servers to the farm, you can manage the farm using the various ctx commands. For example, you can use the ctxappcfg command to publish and configure applications on one or more servers in the farm, and ctxqsession to query servers in the farm.

**Note:** If you used previous versions of XenApp for UNIX, you may notice changes to some ctx commands, particularly for server farms. For example, there is a publish parameter in the ctxappcfg command (that replaces the add parameter) that allows you to publish and configure applications on any server in the farm.
Licensing XenApp for UNIX

XenApp for UNIX uses the *Citrix Licensing* method. This means that you use a license server and, if you use the Citrix License Server for Windows, a user interface for managing licenses, known as the License Management Console. License files are downloaded from the Citrix Web site and stored on the license server.

Citrix Licensing offers many benefits, including the ability to centrally manage and monitor license usage, access your licensing data remotely, and create reports for analyzing trends in license usage. Licenses can be shared across farms, and an electronic backup of all licenses is stored on the Citrix Web site.

To license XenApp for UNIX, you require XenApp Enterprise edition or Platinum edition licenses. These licenses enable all the features available in XenApp for UNIX, including load balancing and client drive mapping. Other edition licenses are not applicable to XenApp for UNIX; upgrade licenses are also not applicable.

**Citrix License Server for UNIX**

A license server that runs on the Solaris platform, rather than on Windows, is available, called the Citrix License Server for UNIX. This license server can be downloaded from the Citrix Web site. For more information about installing and configuring this license server, see the documentation that accompanies the download.

**Coexisting with Earlier Citrix Licensing**

The previous Citrix licensing method, in which base licenses and server extension licenses were installed on each product server, is no longer supported in XenApp for UNIX.

Licenses cannot be shared between Version 4.0 servers and servers running earlier versions. However, servers running Version 4.0 and earlier versions will coexist in a network.

Commands such as ctxqserver -license, that relate to the previous Citrix licensing method, will continue to function for backwards compatibility; however, meaningful results will appear only for servers running XenApp versions prior to Version 4.0.
Licensing XenApp for UNIX: An Overview

To deploy and license XenApp for UNIX, you must complete the following tasks:

1. Install the license server and the License Management Console on a suitable computer. The Windows licensing components and the License Management Console are available on the XenApp installation media.

   **Note:** To run a license server on the Solaris platform, download the Citrix License Server for UNIX from the Citrix Web site. The download includes documentation about installing and configuring this license server. Note that this download does not include the License Management Console.

2. Connect to [http://www.citrix.com](http://www.citrix.com) to download your license files.

3. Copy the license files to your license server.

   **Note:** These tasks are described in detail in *Getting Started with Citrix Licensing*. Citrix recommends that you read this guide before installing XenApp for UNIX.

4. Deploy XenApp for UNIX.

5. If necessary, configure communication between XenApp for UNIX servers and the license server using ctxlsdcfg. This is described in the following topic. However, if you use the installer script to install XenApp for UNIX, the installer script configures communication with the license server for you.
Configuring Communication with the License Server

This topic discusses how to configure XenApp for UNIX to use Citrix Licensing. It explains how to display and specify the license server location and port number using ctxlscfg.

Typically, these communication settings are specified during XenApp for UNIX installation. Sometimes, however, you may need to edit these settings after installation; for example:

- If you decide to install the license server software after you install XenApp
- If you do not use the installer script to install XenApp
- If you rename your license server
- If you transfer the licenses for a server farm to another license server
- If you change the port your license server uses
- If you change a server farm so that it points to another license server
- If you want to change whether XenApp runs in feature pack or hotfix mode
- If you want to change how XenApp for UNIX shares licenses with XenApp for Windows

ctxlscfg is a farm-wide setting, so you need to run this command on only one server in the farm. The settings you specify are propagated automatically throughout the server farm.
To change license server settings for a farm

1. Log on to the server as an administrator.

2. At a command prompt, type ctxlsdcfg.

   The following prompt appears:

   License Config>

3. At the License Config prompt:

   - To specify the license server name, type server server-name where server-name is the name of the license server.

   - To specify the license server port number, type port port-number where port-number is the port number of the license server. By default the port number is 27000.

   - To specify the product edition, type edition product-edition where product-edition is either Enterprise or Platinum depending on which XenApp edition you are licensed to use. By default the product edition is Enterprise.

   - To specify feature pack or hotfix mode, type mode mode where mode is either FeaturePack1 or Base. By default the mode is FeaturePack1 when running XenApp 4.0, with Feature Pack 1.

   - To specify whether XenApp for UNIX servers can share licenses with older or newer versions of XenApp for Windows, type compatibility compatibility where compatibility is 4.0 to allow license sharing with servers running Citrix Presentation Server 4.0 for Windows or earlier, or post4.0 to allow license sharing with servers running Citrix Presentation Server 4.5 or later. By default compatibility is set to post4.0.

     Note: Settings for compatibility and mode options are propagated to all servers in the farm only if Citrix XenApp 4.0, with Feature Pack 1, for UNIX is installed on the Management Service Master server.

4. At the License Config prompt, type exit.

5. At the prompt to save your changes, type y (or yes).
To display license server settings for a farm

1. Log on to the server as an administrator.

2. At a command prompt, type ctxlsdconfig.
   
   The following prompt appears:

   License Config>

3. At the License Config prompt, type list. The current license server settings appear.

4. At the License Config prompt, type exit.
Publishing Applications and Desktops

To a client user, a published application appears similar to an application running locally on the client device.

Published applications:

- Give client users easy access to applications running on servers
- Increase your control over application deployment
- Shield users from the complexities of the UNIX environment hosting the ICA session

The ctxappcfg command is the main tool for publishing applications. You can publish any application that can run on the UNIX workstation or server on which XenApp is installed.
Why Publish Applications?

The main reasons for publishing applications are the ease of user access, the degree of administrative control, and the efficient use of resources.

Administrative Control

When you publish applications, you get greater administrative control over application deployment.

- **Enabling and disabling applications.** You can disable published applications without having to delete their configuration. This allows you to temporarily stop users from connecting to published applications. A disabled application can be quickly enabled at a later stage.

- **Load balancing.** Application publishing lets you direct connection requests to the least busy server in a group of servers configured to run an application.

User Access

When you publish applications, user access to those applications is greatly simplified in the following areas:

- **Addressing.** Instead of connecting to a server by its IP address or server name, client users can connect to a specific application or desktop by whatever name you give it. Connecting to applications by name eliminates the need for users to remember which servers contain which applications. This also allows administrators to change the server(s) on which applications are deployed, without reconfiguring plugins, and without users being aware of the change.

- **Navigation of the server desktop.** Instead of requiring client users to have knowledge of the UNIX desktop to find and start applications after connecting to servers, published applications present the user with only the desired application in an ICA session.

Efficient Use of Resources

ICA connections to server desktops can consume considerable resources because, by default, CDE is loaded for each connection. For more efficient use of server resources, use published applications rather than server desktops.
Publishing Applications for Explicit or Anonymous Use

When you publish an application, you have to specify whether the application is for anonymous or explicit use.

Publishing Applications for Explicit Use

Explicit users have their own user accounts.

If you publish an application for use by explicit users, when the users log on, they supply their user name and password. Explicit users have a “permanent” existence—their desktop and security settings are retained between sessions and their files persist from one session to another.

Publishing Applications for Anonymous Use

Publishing applications for anonymous use allows you to provide “guest” user access to an application.

When a user starts an application published for anonymous use, no logon box appears and the user does not have to supply a user name or password. Instead, the server selects an available account from a pool of anonymous user accounts and assigns this to the user.

A temporary home directory is also assigned to users for use during the session. Users do not have a persistent identity, and no information in the home directory is retained when they log off. Any desktop settings, user-specific files, or other resources created or configured by the user are discarded at the end of the ICA session.

If the session is idle (that is, if there is no user activity for a specified time period), the session is terminated. Users are logged off after a broken connection or time-out.

For information about how to change or maintain anonymous user accounts, see Configuring Anonymous Users.

For information about setting up configuration files for applications published for anonymous use, see Publishing Preconfigured Applications for Anonymous Use.

Note: The total number of users, whether anonymous or explicit, who can be logged on to the server at the same time depends upon your licensed user count. See Getting Started with Citrix Licensing for details.

Security Considerations

Take care when choosing applications to publish anonymously, because no user name or password is required to access these applications and, therefore, little meaningful audit data can be obtained. Citrix recommends that you do not publish applications that will
provide users with a command shell, because they may be able to access and affect the system in the same way as an explicit user.

For example, on HP-UX, users can change their shell or information from a logon shell. Such changes persist even after the session is terminated—that is, if a change is made to an anonymous user account, the next user of this account will pick up these changes. To prevent users from changing their shell, restrict /etc/shells so that it contains only the desired system shell.

If you need to publish applications for explicit use and applications for anonymous use that may present users with a command shell, you can partition the applications onto separate servers and tune the server security so that the server with anonymous applications is more tightly controlled than the server with explicit applications. You may also need to change the permissions on some command-line tools (for example, passwd and chsh) so that members of the ctxanon group cannot execute these tools.
Publishing an Application, Shell Script, or Desktop

These topics explains how to publish applications (including Java and legacy applications), shell scripts, and server desktops. They also explains how to publish applications on UNIX servers of different architecture, change the working directory, and configure the server to accept published application parameters passed by the plugin.
Publishing Applications

Use the ctxappcfg command to publish an application. The command prompts you for the information required to publish the application.

Application installation is not part of the application publishing process. Before an application can be published, both XenApp and the application must be installed. The order in which you install the application and XenApp does not matter. After an application is installed, it can be published at any time.
To publish an application

1. Log on to the server as an administrator.

2. At a command prompt, type ctxappcfg.
   
The following prompt appears:
   
   **App Config>**
   
3. At the App Config prompt, type publish. You are prompted for each item of information you need to supply:

<table>
<thead>
<tr>
<th>At the prompt for</th>
<th>Specify</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name you want to use for the published application. The user selects this name when setting up an ICA connection to this published application. The name does not need to be the same as the name of the executable file for a particular program.</td>
<td>No default</td>
</tr>
<tr>
<td>Command-line</td>
<td>The command line required to run the application or script file; for example: <code>/usr/bin/diary.bin.</code></td>
<td>No default</td>
</tr>
<tr>
<td>Working directory</td>
<td>The default working directory. This directory must exist. Leave blank to specify the user’s home directory. Note that <code>~/sub-dir</code> is supported; <code>~otheruser</code> is not.</td>
<td>User’s home directory</td>
</tr>
<tr>
<td>Anonymous [yes</td>
<td>no]</td>
<td>yes if the application is for anonymous use only, or no if it is for use by users with explicit accounts only.</td>
</tr>
<tr>
<td>Description</td>
<td>An optional description that appears on the user’s Web page. This information is required for applications accessed using the Web Interface.</td>
<td>Blank</td>
</tr>
<tr>
<td>Folder</td>
<td>A folder containing the application. This information is required for applications accessed using the Web Interface.</td>
<td>Blank</td>
</tr>
<tr>
<td>Icon File</td>
<td>The icon file displayed against a published application in the Web Interface.</td>
<td>ICA icon</td>
</tr>
<tr>
<td>Window Size</td>
<td>The window size and type of window. This information is required for applications accessed using the Web Interface. Specify window size as: <code>widthxheight</code>, for example, 1024x768; or % (percentage) of a desktop, for example, 70%. Specify type of window as seamless (the window size is controlled by the plugin) or fullscreen (full screen display).</td>
<td>800 x 600 pixels</td>
</tr>
</tbody>
</table>
**Publishing Applications**

<table>
<thead>
<tr>
<th>Configurations</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Color Depth</strong></td>
<td>The number of colors used to display the application. Choose from 16, 256, 4bit, 8bit, 16bit, and 24bit. This information is required for applications accessed using the Web Interface.</td>
<td>256 colors</td>
</tr>
<tr>
<td><strong>Enable SSL security</strong></td>
<td>Yes to use SSL to secure connections to this application, or no if you do not want to use SSL.</td>
<td>Controlled by default settings</td>
</tr>
<tr>
<td><strong>User name</strong></td>
<td>The user names of users permitted to access this application. Type one user name per line. Leave a blank line to complete the list.</td>
<td>No default</td>
</tr>
<tr>
<td><strong>Group name</strong></td>
<td>The names of user groups or netgroups permitted to access this application. Type one group name per line. Leave a blank line to complete the list. To denote a netgroup, use an @ as the first character of the name; for example @netgroup1.</td>
<td>No default</td>
</tr>
<tr>
<td><strong>Server name</strong></td>
<td>The names of servers in the farm that will publish this application. Type one server name per line. Leave a blank line to complete the list. To specify all current servers in the farm, type an asterisk (*). To specify all current and future servers in the farm, type a plus sign (+).</td>
<td>No default</td>
</tr>
</tbody>
</table>

4. At the App Config prompt, type exit.

**Note:** Increasing window size and color depth increases demand upon memory. For example, an ICA connection configured to run at a color depth of 256 colors and window size of 4096 x 4096 uses approximately 16MB of memory just for the ICA session (additional memory is required for the applications). An ICA connection configured to run at the same window size but at a color depth of 24-bit True Color uses approximately 64MB of memory. Consequently, as memory consumption increases, it may not be possible to run as many concurrent sessions without increasing memory.

If you specify a netgroup, only the presence of a user in a netgroup is checked; the host and domain fields are ignored.

The published application is enabled automatically. You can now connect to the server from a client device and set up a connection to this published application.

You can change the configuration of a published application at any time; see Changing the Settings of a Published Application for more details.

When you first publish an application, you can specify display settings for folder, icon, window size, and color depth. If you do not configure these display settings, default display settings are used. You can change the default display settings for all published applications in the server farm; for more information, see Specifying Default Settings for Published Applications.

Tip: To publish an application for both explicit and anonymous use, publish it under different names—once for explicit use and once for anonymous use.
Publishing a Shell Script

You can also publish an application by writing a script file that sets up the application environment and then executes the application. You then publish the shell script file as a published application, using the ctxappcfg command. To publish a script file, enter the path to and name of the script file at a command prompt.

Publish a shell script if you want to publish an application that requires a particularly complex environment; for example, if you need to set particular environment variables.

To publish a shell script in a server farm, ensure the shell script is present on all the servers in the farm on which you want to publish it.
Publishing a Desktop

You publish a server desktop in the same way you publish an application, using the ctxappcfg command. However, to indicate you are publishing a desktop, you leave the command line blank.

**Note:** ICA connections to server desktops consume considerable server resources because, by default, CDE is loaded for each connection. For more efficient use of server resources, use published applications rather than server desktops.
You can publish Java applications on your server by writing a script file that you publish using the ctxappcfg command. In the script file, include any environment variables required to set up the application environment and the commands to start the Java application.
You can publish applications that require use only of the command line. For example, you may have a legacy application that you want to publish. You do this using the `ctxappcfg` command. At a command prompt, type:

```
xterm -e <path> "commands"
```

where `commands` is the set of commands required to start the application. Enclose the commands within double quotes. If the set of commands is complex, include this in a script file and run the script file:

```
xterm -e <path> script_file
```
You can publish applications on UNIX servers that are of an architecture different from the XenApp server. For example, you can publish an application on a XenApp server, although the application exists and runs on a Linux server.

To do this, you create a script file on the XenApp server to set up the application environment and start the application on the remote server. This script uses the ssh client command to run the script on the remote server.

Finally, you publish the script on the XenApp server using the ctxappcfg command.

**Example**

The following example shows how to publish an application that runs on a Linux server. In this example, the XenApp server is called “Buffy,” the Linux server is called “Mandix,” and the application is called “Diary.”
Step 1 - Create a script file for Buffy

1. Create a script file on Buffy that will set up the application environment and start rundiary.sh on Mandix. For example, create a script file /export/home/apps/diary.sh containing:

```bash
#!/bin/sh
# launch app on the machine "Mandix"
ssh -X Mandix "/usr/local/bin/rundiary.sh ~/group.cal"
```

2. Make sure that the script file works on Buffy, by testing that it correctly launches the application on Mandix, using a display on Buffy. `~/group.cal` is the parameter passed to the Diary application on Mandix.

Step 2 - Publish the application on Buffy

1. Create a script file on Buffy that uses the ctxappcfg command to publish diary.sh. Make sure you include blank lines where appropriate. For example:

   `ctxappcfg <<EOF`

   `EOF`
publish
MY_DIARY
/export/home/apps/diary.sh
-/data
no
My diary application
Applications
/tmp/icon1.xpm
800x600
16bit
no
user1

group1
group2

buffy

EOF

2. Test that the script file works by making an ICA connection to MY_DIARY.
Specifying a Working Directory for Published Applications

By default, when a user connects to a published application, the application starts in the user’s home directory on the XenApp server. However, you can change the directory in which the application runs by specifying a working directory on the client device.

To do this, you publish the application on the server in the usual way, and configure the plugin to pass a working directory parameter to the server.

Example

The following example shows how to configure the published application “Editor” to run in the working directory /home/docs.

Step 1—Publish Editor on the server

1. Install Editor on the XenApp server.

2. Publish Editor in the normal way using the ctxappcfg command.

Step 2—Configure the plugin

1. Create an ICA connection to the Editor application in Program Neighborhood—for example, create an ICA connection and name it “MyEditor.”

2. Locate the APPSRV.ini file and open it in an editor (such as Notepad).

3. In the APPSRV.ini file, find the name of the published application; this is the name you gave the application in Program Neighborhood, contained within square brackets. For example, find: [MyEditor].

4. In the lines relating to the published application, add a line for the working directory (if such a line does not exist already). For example, for the Editor application, add the line:

   WorkDirectory=/home/docs
Publishing an Application to Accept Parameters from the Plugin

You can configure the XenApp server to accept published application parameters passed by the plugin. This allows users to connect to a published application and automatically launch a particular file. For example, if users regularly update a particular document, you can publish the application that they use to automatically open the document specified by the client device.

To do this, you configure the plugin to pass parameters to the server, and configure the server to accept and use the parameters passed by the plugin.

Example

A user wants to regularly update a resume, which is stored in: /home/docs/MyCV.doc, using the published application “Word.” The following shows how to configure the published application to automatically open this file when the user connects.

Step 1—Publish Word on the server

1. Install Word on the XenApp server.

2. Publish Word using the ctxappcfg command. At a command prompt, include “%*” where the parameters from the plugin are to be included. For example:

   /usr/bin/word.bin %*

Step 2—Configure the plugin

1. Create an ICA connection to the Word application in Program Neighborhood; for example, create an ICA connection and name it “MyCV.”

2. Locate the APPSRV.ini file and open it in an editor (such as Notepad).

3. In the APPSRV.ini file, find the name of the published application—this is the name you gave the application in Program Neighborhood, contained within square brackets. For example, find: [MyCV].

4. In the lines relating to the published application, find the line for the initial program. For example:

   InitialProgram=""SERVER1"

5. Edit this line with the file name to be opened. For example:
Publishing an Application to Accept Parameters from the Plugin

InitialProgram=#"SERVER1" /home/docs/MyCV.doc

**Note:** If there is no “%*” in the command line on the server, parameters from the plugin are ignored. If no parameters are passed by the plugin or the syntax is incorrect (for example, the quotes are missing), the server ignores the parameters and “%*” has no effect.

Because plugin parameters are interpreted by the shell, you can use wildcards, environment variables, and so on.

If you specify plugin parameters, seamless session sharing is switched off.
Displaying Published Application Details

You can use ctxappcfg to display all the applications published on the local server or in the server farm. You can then use select to display details about a particular published application.
To display details about the applications published

1. Log on to the server as an administrator.

2. At a command prompt, type ctxappcfg. This starts the program and displays the following prompt:

   App Config>

3. At a command prompt, type list. This displays the names of the applications published on the server or in the server farm:

   App Config> list
   Name: “Accounts”
   Name: “Orders”
   Name: “Diary”

   Applications that are disabled have (disabled) displayed next to them.

4. To find out more details about a particular published application, use the select command with the name, for example:

   App Config> select Diary

   This displays the details for the published application, for example:

   Name: Diary
   Command line: /usr/bin/diary.bin
   Working directory: ~/tmp
   Icon: Inherited from default application settings.
   Anonymous: no
   Enabled: yes
   Description:
   Folder:  
   Window Size: Inherited from default application settings.
   Color Depth: Inherited from default application settings.
   SSL security configuration: Inherited from default application settings.

5. If you want to list information for a different application, type drop to deselect the current application. You can then use the select command again with the appropriate application name.

6. To exit from ctxappcfg, type exit.

Tip: You can also display information about published applications on the network using the ctxqserver command.
Maintaining Published Applications

These topics explain how to change a published application’s settings, configure user access to published applications, and manage the servers that publish applications. They also describe how to configure default settings for all published applications in the server farm.
Changing the Settings of a Published Application

After publishing an application, you can change its settings using the ctxappcfg command. You can change the settings for published applications on the local server or in the server farm.

First, you use the select command to select the application you want to change. Then you use the set command to configure settings, such as the working directory or the application’s description. The set command is described below.

**Note:** After selecting an application, you can also change the icon file displayed against a published application, configure user access to applications, and manage the servers that publish an application. These features are described later in this chapter.
To configure a published application

1. Log on to the server as an administrator.

2. At a command prompt, type ctxappcfg. This starts the program and displays the following prompt:

   App Config>

3. At a command prompt, type list to check the names of the applications published on the server or in the server farm.

4. Select the published application you want to change; for example:

   App Config> select Diary

5. This displays the details for the published application, for example:

   Name: Diary
   Command line: /usr/bin/diary.bin
   Working directory: ~/tmp
   Icon: Inherited from default application settings.
   Anonymous: no
   Enabled: yes
   Description:
   Folder:
   Window Size: Inherited from default application settings.
   Color Depth: Inherited from default application settings.
   SSL security configuration: Inherited from default application settings.

6. To change the configuration, use the set command. This has the following syntax:

   set [cmd={cmd_line}, dir={dir_name}, anonymous={yes|no}, enabled={yes|no}, description={description}]

   —Or—

   set server={server_name}, [cmd={cmd_line}, dir={dir_name}]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cmd</td>
<td>The command line required to run the application or script file; for example, /usr/bin/diary.bin.</td>
</tr>
<tr>
<td>dir</td>
<td>The default working directory. This directory must exist. Leave blank to specify the user’s home directory. Note that ~sub-dir is supported; ~otheruser is not.</td>
</tr>
</tbody>
</table>
### Changing the Settings of a Published Application

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>anonymous</td>
<td>Type yes if the application is for anonymous use only, or no if it is for use by users with explicit accounts only.</td>
</tr>
<tr>
<td>enabled</td>
<td>Type no to disable an application—this stops users from connecting to the application without you having to delete its configuration. Type yes to enable a previously disabled application.</td>
</tr>
<tr>
<td>description</td>
<td>The description displayed on the user’s Web page. If the description includes spaces, enclose it within quotes. This information is required for applications accessed using the Web Interface.</td>
</tr>
<tr>
<td>folder</td>
<td>The name of a folder containing the program that the Web Interface displays.</td>
</tr>
<tr>
<td>window_size</td>
<td>The window size and type of window that the Web Interface displays. Specify window size as: widthxheight, for example, 1024x768; or % (percentage) of a desktop, for example, 70%. Specify type of window as seamless (the window size is controlled by the plugin) or fullscreen (full screen display).</td>
</tr>
<tr>
<td>color_depth</td>
<td>The number of colors used to display the application in the Web Interface. Specify 16, 256, 4bit, 8bit, 16bit, or 24bit.</td>
</tr>
<tr>
<td>ssl_enabled</td>
<td>Specifies whether or not SSL is used to secure connections to the application. Type yes to use SSL, or no if you do not want to use SSL.</td>
</tr>
<tr>
<td>server</td>
<td>To change the settings on a particular server only, specify a server name. This option applies only to the command line and working directory.</td>
</tr>
</tbody>
</table>

7. To save your changes, type save.

8. To exit from ctxappcfg, type exit.
Displaying and Changing the Icon File

Use ctxappcfg to find out which icon is currently displayed against a published application when the application is accessed using the Web Interface.

Use the export icon command to save the icon to a file. You can later view this file using a suitable tool. Use the import icon command to specify a new icon for the published application.

By default, the ICA icon appears. However, you can specify another icon to use for a published application. The icon you specify must be:

- A graphic in .xpm (X pixmap) format.
- 32 x 32 pixels. If your icon is larger than this, use an image editor to resize it to the correct size.
To display or change the icon used for a published application

1. Log on to the server as an administrator.

2. At a command prompt, type ctxappcfg. This starts the program and displays the following prompt:

   App Config>

3. At a command prompt, type list to check the names of the applications published on the server or in the server farm.

4. Select the published application you want; for example,

   App Config> select Diary

5. This displays the details for the published application; for example,

   Name: Diary
   Command line: /usr/bin/diary.bin
   Working directory: ~/tmp
   Icon: Inherited from default application settings.
   Anonymous: no
   Enabled: yes
   Description: 
   Folder: 
   Window Size: Inherited from default application settings.
   Color Depth: Inherited from default application settings.
   SSL security configuration: Inherited from default application settings.

   To | Type
   ---|---------------------
   Export the current icon to a file that you can later view. You are prompted for the file name. | export icon
   Specify a different icon file for the published application. You are prompted for the file name. | import icon

6. To save your changes, type save.

7. To exit from ctxappcfg, type exit.
Specifying Default Settings for Published Applications

You can configure default settings for all published applications in the server farm using the ctxappcfg command. You can configure:

- Default display settings for applications accessed using the Web Interface. These settings include folder name, window size, and color depth. These settings affect only applications accessed using the Web Interface, not applications accessed using a direct client connection where display settings are controlled by the plugin.

- SSL secure connections to applications.
To change the default settings for all published applications

1. Log on to the server as an administrator.

2. At a command prompt, type ctxappcfg. This starts the program and displays the following prompt:

   App Config>

3. At a command prompt, type default. The default settings appear; for example,

   App Config> default
   Icon: Not configured.
   Description:
   Folder:
   Window Size: 800x600
   Color Depth: 256 colors
   SSL security enabled: no

4. To change the default settings, use the set command, which has the following syntax:

   set [folder={folder name}, window_size={window size}, color_depth={color depth}, ssl_enabled={yes|no}]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>folder</td>
<td>The name of a folder containing the published application. This is used by the Web Interface, which can organize applications into logical folders.</td>
</tr>
<tr>
<td>window_size</td>
<td>The window size and type of window that the Web Interface displays. Specify window size as: widthxheight, for example, 1024x768; or % (percentage) of a desktop, for example, 70%. Specify type of window as seamless (the window size is controlled by the plugin) or fullscreen (full screen display).</td>
</tr>
<tr>
<td>color_depth</td>
<td>The number of colors used to display the application. Choose from 16, 256, 4bit, 8bit, 16bit, and 24bit.</td>
</tr>
<tr>
<td>ssl_enabled</td>
<td>Specifies whether or not SSL is used to secure connections to the application. Type yes to use SSL, or no if you do not want to use SSL.</td>
</tr>
</tbody>
</table>

   **Note:** You cannot display the default icon using ctxappcfg; however, you can use the export icon command to save the icon to a file that you can later view using a suitable tool.

5. To save your changes, type save.

6. To exit from ctxappcfg, type exit.
Configuring User Access to Published Applications

You can configure which users and groups of users can access a published application using the ctxappcfg command.

For each application, the Citrix XML Service stores a list of groups and users for whom the application is visible. The Citrix XML Service for UNIX uses the same users and groups as the XenApp server and the underlying UNIX operating system.

You can display the users and groups allowed to access a published application using the list users and list groups commands. You can also add users and groups who are allowed to access an application, and prevent access to an application using the add users, add groups, remove users, and remove groups commands.

You can add netgroups in addition to normal groups. To denote a netgroup, use an at symbol (@) as the first character of the name; for example, @netgroup1. Note that only the presence of a user in a netgroup is checked; the host and domain fields are ignored.
To configure access to an application

1. Log on to the server as an administrator.

2. At a command prompt, type ctxappcfg. This starts the program and displays the following prompt:

   App Config>

3. At a command prompt, type list to check the names of the applications published on the server or in the server farm.

4. Select the published application you want to display information about; for example,

   App Config> select Diary

   This displays the details for the published application.

<table>
<thead>
<tr>
<th>To</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the users who are allowed to access the published application.</td>
<td>list users</td>
</tr>
<tr>
<td>Display the groups of users who are allowed to access the published application.</td>
<td>list groups</td>
</tr>
<tr>
<td>Add users who are allowed to access the published application. Type one user name per line. Leave a blank line to complete the list.</td>
<td>add users</td>
</tr>
<tr>
<td>Add groups of users or netgroups who are allowed to access the published application. Type one group per line. Leave a blank line to complete the list. To denote a netgroup, use an @ as the first character of the name; for example, @netgroup1.</td>
<td>add groups</td>
</tr>
<tr>
<td>Prevent particular users from accessing the published application. Type one user name per line. Leave a blank line to complete the list.</td>
<td>remove users</td>
</tr>
<tr>
<td>Prevent groups of users from accessing the published application. Type one group per line. Leave a blank line to complete the list.</td>
<td>remove groups</td>
</tr>
</tbody>
</table>

5. To save your changes, type save.

6. To exit from ctxappcfg, type exit.
Managing the Servers that Publish an Application

You can display the servers in a farm that publish an application using ctxappcfg with the list servers command. You can also publish an application on one or more servers in the farm using the add servers command.

Note: Ensure the application is installed on a server before you attempt to publish it. After an application is installed, it can be published at any time.

To remove a published application from particular servers in the farm, you use the remove servers command. This removes the application only from the servers you specify; the application remains on other servers in the farm. If you want to completely remove a published application from all servers in the farm, use the delete command.
To manage the servers that publish an application

1. Log on to the server as an administrator.

2. At a command prompt, type ctxappcfg. This starts the program and displays the following prompt:

   App Config>

3. At a command prompt, type list to check the names of the applications published on the server or in the server farm.

4. Select the published application you want to display information about; for example,

   App Config> select Diary

   This displays the details for the published application.

<table>
<thead>
<tr>
<th>To</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display all servers in the farm that publish the application.</td>
<td>list servers</td>
</tr>
<tr>
<td>Publish the application on another server in the farm. Type one server name per line. Leave a blank line to complete the list. To specify all current servers in the farm, type an asterisk (*). To specify all current and future servers in the farm, type a plus sign (+).</td>
<td>add servers</td>
</tr>
<tr>
<td>Remove the published application from one or more servers in the farm. Type one server name per line. Leave a blank line to complete the list.</td>
<td>remove servers</td>
</tr>
</tbody>
</table>

5. To exit from ctxappcfg, type exit.
Deleting a Published Application from All Servers

Deleting a published application removes all published application configuration information from all servers in the farm. When you delete a published application, that application is no longer available to client users under the published application name (although it may be available as another published application or from a server desktop session).

Tip: To temporarily stop users from connecting to a published application, disable the published application. Disabling a published application does not delete its configuration, and it can be quickly enabled at a later stage.

If you want to make the application available again, republish it under its old name or with a new name.

To delete a published application from the farm

1. Run ctxappcfg. At a command prompt, type list to display the names of the applications published on the server.

2. Select the published application you want to delete; for example,

   
   App Config> select Diary

3. Type delete.

4. Confirm the deletion by typing y.

5. Type exit.
Enabling and Disabling Published Applications

You can disable a published application without having to delete its configuration. This is useful when you want to temporarily stop users from connecting to a published application; for example, to upgrade the application to a newer version or to apply patches. A disabled application can be quickly enabled at a later stage.

When you disable a published application, users can no longer see or connect to the disabled application on any of the servers in the farm.

Note: When you publish an application, it is enabled by default.

To enable or disable a published application

1. Use the ctxappcfg utility with the set command.

2. Set the enabled option to no to disable an application, or set it to yes to enable a previously disabled application.
Creating a New Published Application from Existing Details

After you publish an application, you can reuse the settings by copying the details to a new name.

**To copy details to create a new published application**

1. Log on to the server as an administrator.

2. At a command prompt, type ctxappcfg. This starts the program and displays the following prompt:

   App Config>

3. At a command prompt, type list to check the names of the applications published on the server.

4. Select the published application that has the details you want to copy; for example,

   App Config> select Diary

   This displays the details for the published application.

5. Type copy and the new name for the published application at the prompt.

6. Type drop.

7. Change the details for the new published application using the set command.

8. When you are finished configuring the published application, type save to save the changes.

9. To exit from ctxappcfg, type exit.
Renaming a Published Application

After you publish an application, you can change its name by copying the settings to a new name and then deleting the original.

To rename a published application

1. Log on to the server as an administrator.
2. At a command prompt, type ctxappcfg. This starts the program and displays the following prompt:

   App Config>

3. At a command prompt, type list to check the names of the applications published on the server.
4. Select the published application you want to rename; for example,

   App Config> select Diary

   This displays the details of the published application.
5. Type copy and the new name for the published application at the prompt.
6. Type drop.
7. To delete the original published application settings, select the original application and use the delete command.
Restricting Connections to Published Applications Only

You can restrict users so that they can connect only to published applications on a server. Doing so prevents users from connecting to a server by name or to the server desktop.

Because connections to server desktops consume considerable server resources, restricting users to published applications makes more efficient use of resources.

To restrict connections to published applications only

1. Log on to the server as an administrator.

2. Use the ctxcfg command to allow users to run only published applications:

   `ctxcfg -i PUBONLY`

Note: To restrict access on several servers, you must run ctxcfg -i PUBONLY at each server.
Configuring an Initial Program

An initial program is an application that XenApp starts automatically when a user logs on. Closing the initial program does not terminate the ICA session.

Initial programs:

- Can be set on the server by an administrator.
- Can be set from a client device as part of the properties for a specific connection. If an initial program is configured on the server and client device, the initial program configured on the server is started when a user logs on.

**To configure an initial program on the server**

1. Log on to the server as an administrator.
2. At a command prompt:

<table>
<thead>
<tr>
<th>To</th>
<th>Use the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the server so that if an initial program is set on the client device, it is used.</td>
<td><code>ctxcfg -i INHERIT</code></td>
</tr>
<tr>
<td>Configure the server to start the initial program <em>programe</em> whenever a user connects, where <em>wd</em> is the working directory.</td>
<td><code>ctxcfg -i prog=programe,wd=dir</code></td>
</tr>
<tr>
<td>List the current initial program details.</td>
<td><code>ctxcfg -i list</code></td>
</tr>
</tbody>
</table>
Publishing Preconfigured Applications for Anonymous Use

When a user logs on to use an application that you published for anonymous use, the user is assigned an empty home directory. When the user logs off, any files that the user creates in this directory are deleted.

Some applications use configuration files that initialize settings when the application starts. For example, an application such as a Web browser may use proxy settings, file paths, and font and display settings. In normal use, a user configures these settings once. If the configuration files are not available, the application starts in its default configuration.

You can set up configuration files for applications that you publish for anonymous use. You create these in a special template directory called /usr/anon/anontmpl. When a user logs on, all files in the template directory are copied to the assigned home directory.
To create configuration files for an application

1. Create a user (for example, called “anontmpl”) with home directory set to /usr/anon/anontmpl. Use this user account only to preconfigure applications for anonymous use.

2. Log on to the server as this user and run the application you want to configure.

3. Configure the application so that it mirrors the settings you want to provide when an anonymous user logs on. For example, for a Web browser application such as Netscape, you may want to set proxy server settings or clear the cache.

4. Exit the application.

5. Start the application again and make sure that the application works as required. If not, adjust the process and repeat until you are sure that the correct configuration is in use when the application starts.

6. Using grep or a text editor, search for occurrences of the user name or folder name (in this example, “anontmpl”) in each of the files in /usr/anon/anontmpl.

7. Make the template directory readable by everyone using:

   chmod -R a+rX

8. Log on as an administrator.

9. Edit the script file ctxanoninit.sh. This file is installed in the following directory:

   On HP-UX and Solaris:

   /opt/CTXSmf/lib

   On AIX:

   /usr/lpp/CTXSmf/lib

10. For each file containing occurrences of “anontmpl” in the files in /usr/anon/anontmpl, add lines to the end of ctxanoninit.sh that use the sed command to substitute the user name and home directory.

    For example, a Netscape preferences file contains references to the home directory, so add the following lines to the end of ctxanoninit.sh:

    ```
    sed -e "s,anontmpl,$USER,g" $ANON_TMPL_DIR/.netscape/preferences.js > newprefs.js
    rm .netscape/preferences.js
    mv newprefs.js .netscape/preferences.js
    # add commands here to set the correct file permissions.
    ```
Note: Use the environment variable $USER, which is set automatically by /bin/sh, to determine the name to substitute.

11. Publish the application for anonymous use. Make sure that the application works by launching a session from a client device, repeating the above steps as necessary.
Managing Servers, Users, and Sessions

These topics describe how to manage the users, sessions, and processes on a XenApp server. and include information about how to:

- Display information about sessions and users
- Display information about the servers on the network
- Log off, disconnect, and reconnect sessions
- Reset sessions in case of error
- Shadow ICA sessions
- Send messages to users on your server
- Display available client printers and print files from the command line or from applications
- Connect to a remote server from within an ICA session
Displaying Information about Users and Sessions

You can display information about connections to one or more XenApp servers in a farm. This includes information about the users who are connecting and session details, such as the session id and session state.

To display a default listing of session details, use the ctxqsession command. To display a similar listing, ordered by user name, use the ctxquser command. If you require more information about sessions, such as the X display number, or you want to display information in a format that differs from the default listing, use the ctxquery command. You can also use ctxquery to produce machine-readable output. These commands are described in the following topic.

To display session details

Run the ctxqsession command:

<table>
<thead>
<tr>
<th>To</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display sessions on the local server</td>
<td>ctxqsession</td>
</tr>
<tr>
<td>Display sessions on another server in the farm</td>
<td>ctxqsession -s servername where servername is the name of the server you want to query</td>
</tr>
<tr>
<td>Display sessions on all the servers in the farm</td>
<td>ctxqsession -S</td>
</tr>
</tbody>
</table>

A list similar to the following appears:

```
   Terminal
   Window   Edit   Options   Help
   grumblyx  ctxqsession SESS:ID  USERNAME  STATE  TYPE  DEVICE
   grumbly:0  0       ctxsrvr     listen  wdica  -
   grumbly:1  1       ctxsrvr     disc    wdica  MANDY1
   grumbly:2  2       mandyl      active  wdica  MANDY1
   grumbly:3  3       emmar       active  wdica  BUUFFUFF
   grumblyx
   grumblyx
```

To display session details, by user name

Run the ctxquser command:

<table>
<thead>
<tr>
<th>To</th>
<th>Type</th>
</tr>
</thead>
</table>
## Displaying Information about Users and Sessions

| Display all user sessions on the local server | ctxquser |
| Display a specific user session on the local server | `ctxquser user username` where `username` is the name of the user you want to query |
| Display all user sessions on another server in the farm | `ctxquser -s servername` where `servername` is the name of the server you want to query |
| Display a specific user session on another server in the farm | `ctxquser -s servername user username` where `servername` is the name of the server and `username` is the name of the user you want to query |
| Display all user sessions on all the servers in the farm | `ctxquser -S` |
| Display a specific user session on all the servers in the farm | `ctxquser -S user username` where `username` is the name of the user you want to query |

A list similar to the following appears:

![Terminal](image)
Displaying More Details or Details in a Different Format

You can display more information about users and sessions than ctxquser or ctxqsession can provide, using the ctxquery command. For example, you can use ctxquery to display the X display number or the name of a published application. You can also use ctxquery to configure the display format. This is useful if you require information in a format other than the default provided by ctxquser or ctxqsession; for example, to display fields in a particular order or produce machine-readable output.

ctxquery has the following syntax:

\[\text{ctxquery} \text{-f short\_format\_options} \text{ | -o long\_format\_options} \text{ | [-m] | [-S | -s server\_name user user\_name]}\]

You can use ctxquery to display information about sessions and users using the -S | -s server\_name user user\_name options, in the same way as you do using ctxqsession and ctxquser. For information about using these options, refer to the ctxquser and ctxqsession commands.

This topic discusses how to configure the display format using the -f short\_format\_options and -o long\_format\_options. With these options, you input either characters or keywords, respectively, to produce your listing. The commands generate the same information so it is a matter of preference as to which one you choose. The use of ctxquery is illustrated in the following example.

**Example**

To locate a user called “Fred,” the X display number he is using, and the published application he launched, type:

\[\text{ctxquery -o user,\text{id,\text{state,xdpy,app} user fred} \text{| -f uiSxp user fred}}\]

Tip: For additional examples of how to use ctxquery, see the ctxquery man page.

**Producing Machine-Readable Output**

You can use ctxquery with the -m option to produce machine-readable output. This alters the column headers to remove spaces so that a constant number of columns appears on every line, making the output machine-readable. For example:
Displaying More Details or Details in a Different Format

ctxquery -f ui$xp user fred -m
About the Display

The following table shows the information displayed by the ctxqsession, ctxquser, and ctxquery commands. It also shows the keywords and characters you can use to configure the display format with ctxquery.

<table>
<thead>
<tr>
<th>Display</th>
<th>Description</th>
<th>ctxquery -o option</th>
<th>ctxquery -f option</th>
</tr>
</thead>
<tbody>
<tr>
<td>SESSION</td>
<td>This is in the format servername:id, where servername is the name of a server in the farm, and id is the session identifier. For example, server1:34 means session 34 running on server1.</td>
<td>id</td>
<td>i</td>
</tr>
<tr>
<td>SESSION NUMBER</td>
<td>The session id number only. Use this to display the session number without the “servername:” prefix.</td>
<td>sess#</td>
<td>N</td>
</tr>
<tr>
<td>SESSION NAME</td>
<td>The session name; for example, tcp#41.</td>
<td>sess</td>
<td>n</td>
</tr>
<tr>
<td>USERNAME</td>
<td>The name of the user.</td>
<td>user</td>
<td>u</td>
</tr>
<tr>
<td>STATE</td>
<td>listen—indicates the session that is listening for new incoming connections.active—indicates an established, active connection.connq—indicates a brief session initialization phase that occurs before the logon prompt appears, and during reconnect.init—a brief session initialization phase.connq—indicates a session that is being connected.discard—indicates a disconnected session.down—indicates a broken session.shadow—indicates that the user of this session is shadowing another.init—a brief session initialization phase.</td>
<td>state</td>
<td>S</td>
</tr>
<tr>
<td>TYPE</td>
<td>wdica—indicates that the ICA protocol is being used.</td>
<td>type</td>
<td>t</td>
</tr>
<tr>
<td>DEVICE</td>
<td>The name of the client device.</td>
<td>dev</td>
<td>d</td>
</tr>
<tr>
<td>IDLE TIME</td>
<td>The length of time since there was user activity in this session. It may take some time to display this, depending on the number of users and how they are distributed across servers.</td>
<td>idle</td>
<td>I</td>
</tr>
<tr>
<td>LOGON TIME</td>
<td>The time the user logged on to the system.</td>
<td>logon</td>
<td>I</td>
</tr>
<tr>
<td>CLIENT ADDRESS</td>
<td>The IP address of the client device.</td>
<td>addr</td>
<td>a</td>
</tr>
<tr>
<td>APPLICATION NAME</td>
<td>The name of the published application.</td>
<td>app</td>
<td>p</td>
</tr>
<tr>
<td>SERVER NAME</td>
<td>The name of the server in the farm.</td>
<td>srvr</td>
<td>s</td>
</tr>
<tr>
<td>DISPLAY</td>
<td>The X display number. To display this without the “:” prefix using ctxquery, use a capital X.</td>
<td>xdpYXdpY</td>
<td>xx</td>
</tr>
</tbody>
</table>
Displaying Information about Servers on the Network

Use the ctxqserver (query server) command to display information about servers on the subnet. You can display information such as server name and network address, transport protocol, and the number of connections available.

**To display information about all servers on the subnet**

At a command prompt, type:

```bash
ctxqserver
```

**To display information about a specific server**

At a command prompt, type `ctxqserver` and specify the server name:

```bash
ctxqserver server-name
```

---

### About the Display

The `ctxqserver` command displays:

<table>
<thead>
<tr>
<th>Display</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>The server name.</td>
</tr>
<tr>
<td>Transport</td>
<td>The transport protocol; that is TCP/IP.</td>
</tr>
<tr>
<td>Conns</td>
<td>The current number of ICA connections on the server.</td>
</tr>
<tr>
<td>Free</td>
<td>The remaining number of connections the server is capable of receiving.</td>
</tr>
</tbody>
</table>
Displaying Information about Servers on the Network

<table>
<thead>
<tr>
<th>Total</th>
<th>The current number of ICA connections plus the number of free connections.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Address</td>
<td>The IP address of the server. An M next to the IP address indicates that the server is the master browser.</td>
</tr>
</tbody>
</table>

**Note:** You can use ctxqserver to display information specific to XenApp servers (such as ICA gateways), or about published applications and sessions on the subnet. You can also use ctxqserver to send requests to servers.

If the server has more than one network interface card (NIC) and you configured it so that the ICA browser listens on only one subnet, ctxqserver displays information only about this one subnet.
Ending a Session

To end a session, you can use commands that either log off or disconnect the session. You can log off or disconnect sessions on the local server or on other servers in the farm.

- Disconnecting a session terminates the connection between the server and client device. However, the user is not logged off, all running programs remain active, and the user can later reconnect to the disconnected session.

- Logging off a session terminates the connection and all running programs, and the user cannot reconnect to the session.
Logging off from a Session

Use the ctxlogoff command to log off from a session.

To log off from your own session

1. Type ctxlogoff.

To log off another user’s session

1. Log on to the server as an administrator.

2. At a command prompt, type ctxqsession to display sessions on the local server or in the farm.

3. From the results of ctxqsession, identify the session id of the connection session you want to forcibly log off.

   Note: You must specify a session identifier. Session names are no longer supported.

4. At a command prompt:

<table>
<thead>
<tr>
<th>To</th>
<th>Use the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log off a session on the local server</td>
<td>ctxlogoff id</td>
</tr>
<tr>
<td>Log off a session on another server in</td>
<td>ctxlogoff servername:id, where servername is the name of a server in the farm, and id is the session identifier. For example, server1:34 means session 34 running on server1.</td>
</tr>
<tr>
<td>the farm</td>
<td></td>
</tr>
</tbody>
</table>
Disconnecting a Session

Use the ctxdisconnect command to disconnect a session.

To disconnect your own session

1. Close the plugin or type ctxdisconnect at a command prompt.

To disconnect another user’s session

1. Log on to the server as an administrator.

2. At a command prompt, type ctxqsession to display sessions on the local server or in the farm.

3. From the results of ctxqsession, identify the session id of the session you want to disconnect.

   Note: You must specify a session identifier. Session names are no longer supported.

4. At a command prompt:

<table>
<thead>
<tr>
<th>To</th>
<th>Use the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disconnect a session on the local server</td>
<td>ctxdisconnect id</td>
</tr>
<tr>
<td>Disconnect a session on another server in the farm</td>
<td>ctxdisconnect servername:id, where servername is the name of a server in the farm, and id is the session identifier. For example, server1:34 means session 34 running on server1.</td>
</tr>
</tbody>
</table>

If a user logs on to the server and there is a disconnected session on the server belonging to that user, the user is given a choice of whether to connect to the disconnected session or start a new session.

Note: You cannot disconnect an anonymous user session because you cannot reconnect to the session when the identity of the user is unknown. If an anonymous session is disconnected, the session is logged off.
Connecting to a Disconnected Session

Use the ctxconnect command from within an ICA session to reconnect to a disconnected session on the local server.

A user can connect to a previously disconnected session by logging on again with the same user name. Once logged on, if there are disconnected sessions on the server, the user can reconnect to the disconnected session or start a new session.

An administrator can connect to any user’s session. Other users can connect only to their own sessions.

To connect to a disconnected session

1. At a command prompt, type ctxqsession to display current sessions on this server. A disconnected session shows disc in the State field.

2. From the results of the ctxqsession command, identify the session id associated with the session to which you want to connect.

3. At a command prompt from within an ICA session, type:

   ctxconnect id

   where id is the session id of the session to which you want to connect.

The server disconnects your current session and connects you to the selected session.

Note: Your connected session must be capable of supporting the video resolution used by the disconnected session. If the session does not support the required video resolution, the operation fails.
Reseting a Session

You can reset a session in the event of an error using the ctxreset command. You can reset a session on the local server or another server in the farm. The system will attempt to terminate all processes running within that session. Resetting a session may cause applications to close without saving data.

To reset a session

1. Log on to the server as an administrator.

2. At a command prompt, type ctxqsession to display sessions on the local server or in the farm.

3. From the results of ctxqsession, identify the session id you want to reset.
   
   **Note:** You must specify a session identifier. Session names are no longer supported.

4. At a command prompt:

<table>
<thead>
<tr>
<th>To</th>
<th>Use the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset a session on the local server</td>
<td>ctxreset id</td>
</tr>
<tr>
<td>Reset a session on another server in the farm</td>
<td>ctxreset servername:id, where servername is the name of a server in the farm, and id is the session identifier. For example, server1:34 means session 34 running on server1.</td>
</tr>
</tbody>
</table>
Reconnecting to Load Balanced Sessions

Published applications allow users to run applications or access a desktop session without knowing the name or address of a particular server. If the published application is located on a single server, users can disconnect and reconnect to the same session.

If the published application is configured to run on multiple servers, users must be reconnected to the same server to reconnect to their session. The ICA browser can reconnect users to their previous session on the same server under certain conditions.

For a user to reconnect to disconnected load balanced sessions:

- The user must disconnect gracefully from the server; for example, by using ctxdisconnect
- The user must reconnect from the same client device (using the same client device name)

Use ctxqsession to view a list that displays disconnected sessions.

**Note:** If users frequently disconnect and reconnect their sessions rather than logging off, the number of sessions on a server farm may not be evenly distributed because users are reconnected to their previous sessions on the same servers.
Shadowing a User’s Session

You can monitor the actions of users, and interact with their sessions, using the keyboard and mouse. This is called shadowing. The person who issues the ctxshadow command is called the shadower, and the session being shadowed is called the shadowed session.
Starting Shadowing

Use the ctxshadow command to shadow another user’s session:

```
ctxshadow {id | servername:id} [-v] [-h[a][c][s]+][x]
```

The ctxshadow command is a user command, rather than a system administration command. Therefore, any user can shadow any other session, provided the shadowed user approves the shadowing, and XenApp security permits the user to shadow. Disabling shadowing notification means that a user may be unaware that shadowing is occurring.

**Note:** The following procedure assumes that you will use the CTRL+* (asterisk) hotkey combination to end shadowing. If you cannot use this hotkey combination, or you want to use an alternative combination to end shadowing, see *Ending Shadowing*.

**To start shadowing a session**

1. Log on to an ICA session.

2. At a command prompt, type ctxqsession to display the current sessions on this server.

3. From the results of the ctxqsession command, identify the session id of the user’s session that you want to shadow.

   **Note:** You must specify a session identifier. Session names are no longer supported. You cannot shadow a session on another server.

4. At a command prompt, type ctxshadow and specify a session id. Use the -v (verbose) argument to display more information during the shadow session initiation; for example:

   ```
   ctxshadow server1:5 -v
   ```

The user is notified of the pending shadowing, and is given the opportunity to allow or deny the shadowing (unless notification was disabled for shadowing using ctxcfg). If the user does not respond to the notification message, the shadow request times out and is terminated.
About Shadowing and the Clipboard

The user of the shadowed session can use the clipboard to copy and paste between the session and applications running locally. As shadower, you cannot access the contents of the shadowed session’s clipboard—information in the clipboard belongs to the shadowed session. However, if you copy information to the clipboard while shadowing, this information is available to the shadowed session for pasting.
Ending Shadowing

By default, you can end shadowing using the CTRL+* (asterisk) hotkey combination.

**To end the shadowing session**

1. Press CTRL+* (asterisk) key of your keyboard’s numeric keypad.

**To configure a different hotkey to end shadowing**

If you cannot use the default hotkey combination from the client device you are using or you prefer to use an alternative, you can configure your own combination. You do this using the ctxshadow command.

The hotkey you configure applies only to the current shadowed session and therefore needs to be set up each time you shadow a session.

1. Log on to an ICA session.
2. At a command prompt, type ctxqsession to display current sessions.
3. From the results of ctxqsession, identify the session id of the user’s session that you want to shadow.
4. At a command prompt, type:

   ```
   ctxshadow {id | servername:id} [-h [[a][c][s]+]x
   ```

   where [a][c][s] and x is the hotkey combination you want to use to end shadowing—choose this combination from:

   - [a][c][s] a = ALT; c = CTRL; s = SHIFT Note: you can use any combination of a, c and s, including all or none.
   - x Choose from the alphanumeric characters: a to z (or A to Z) and 0 to 9.

**Example**

To begin shadowing, and to specify a hotkey combination of ALT+q to stop shadowing the session, type:

```
ctxshadow server1:5 -h a+q
```

**Note:** The hotkey combination is not case-sensitive; therefore, in the above example, you could choose ALT+Q or ALT+q to stop shadowing.
Sending Messages to Users

You can send a message to users using the ctxmsg command. A message can be sent to a particular session or to all sessions, either on the local server or in the entire server farm.

Tip: If a message includes spaces or any other characters that have a special meaning in your UNIX shell, enclose all the text in double quotes.

To send a message to users

1. Log on to the server as an administrator.

2. If you want to send a message to particular sessions, use ctxquser to display the current sessions. From the results of ctxquser, identify a session id for the users and sessions you want to send a message to.

   Note: You must specify a session identifier. Session names are no longer supported.

3. At a command prompt:

<table>
<thead>
<tr>
<th>To</th>
<th>Use the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send a message to a session on the local server.</td>
<td>ctxmsg id message, where id is the session identifier.</td>
</tr>
<tr>
<td>Send a message to a session on another server in the farm.</td>
<td>ctxmsg servername:id message, where servername is the name of a server in the farm, and id is the session identifier. For example, server1:34 means session 34 running on server1.</td>
</tr>
<tr>
<td>Send a message to all sessions on a particular server.</td>
<td>ctxmsg -s servername message, where servername is the name of a server in the farm.</td>
</tr>
<tr>
<td>Send a message to all sessions on the local server.</td>
<td>ctxmsg -a message</td>
</tr>
<tr>
<td>Send a message to all sessions on all servers in the farm.</td>
<td>ctxmsg -S message</td>
</tr>
<tr>
<td>Send a message that includes a time-out period, in seconds. The message appears on the user’s screen until it times out or the user dismisses it.</td>
<td>ctxmsg id message timeout</td>
</tr>
<tr>
<td>Send a message that will suspend your terminal window until the message times out or is dismissed by the user. Note that a command prompt appears only when the user responds or the message times out.</td>
<td>ctxmsg -w id message timeout</td>
</tr>
</tbody>
</table>
Examples

ctxmsg 11 Hello

ctxmsg server1:34 “Happy Birthday”

ctxmsg 5 “Fancy lunch?” 30

ctxmsg -w server1:34 “Are you at your desk?” 60

ctxmsg -S “Get out, the building is on fire”

Tip: To inform users that the server is about to shut down, use the message option with
the ctxshutdown command.
This topic describes the information your plugins need to know when they want to print. It explains how users can list available client printers and print files from a command prompt or from applications.

In the UNIX environment, the application performs the print rendering. The print driver is specified inside the application or, in the case of a desktop utility, raw unformatted text is generated.
Displaying Client Printers or Printer Ports

When a client device connects to a server, client printers are mapped and are available from the desktop command line and from applications running in the session.

From a session, users can list the mapped client printers or available printer ports using the ctxprinters command.

To display mapped client printers

At a command prompt, type:

ctxprinters

A list of printers configured on the client device and mapped for use from the ICA session appears.

(default) appears after the printer that is the default. The following information is shown for each printer:

- Printer name or printer port (for example, lpt1). This can be used in the ctxlpr -P command to specify a printer other than the default.
- Printer driver name. This is for information only.
- Printer connection description. This is for information only.
Printing from a Command Line

Within an ICA session, users can print a file from the command line by using ctxlpr, instead of lpr or lp. If no files are specified, the ctxlpr command takes its input from standard input (stdin).

To print a file from an ICA session

1. At a command prompt, type ctxprinters.

2. From the results of ctxprinters, identify the printer or printer port that you want to use. To print to a printer other than the default, note the printer name (the printer name is the first item in the ctxprinters listing).

3. At a command prompt:

<table>
<thead>
<tr>
<th>To</th>
<th>Use the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Print the file named filename to the default printer.</td>
<td>ctxlpr filename</td>
</tr>
<tr>
<td>Print a series of files to the default printer. Each file is treated as a separate print job.</td>
<td>ctxlpr filename filename</td>
</tr>
<tr>
<td>Print a file to a printer (or printer port) other than the default. This is the printer name or printer port shown in the first column of the output from ctxprinters.</td>
<td>ctxlpr -P [Printername</td>
</tr>
<tr>
<td>Print a file in the background.</td>
<td>ctxlpr -b filename</td>
</tr>
<tr>
<td>Print a file only if the printer is not in use. Use this option to stop an application waiting while other printer jobs are handled. If the printer is in use, an error message appears.</td>
<td>ctxlpr -n filename</td>
</tr>
</tbody>
</table>

Examples

To send the file mydoc.ps to the printer \PRINTSRVR\Sales_HP4000, use the following command:

cctxlpr -P \PRINTSRVR\Sales_HP4000 mydoc.ps

Note: In some UNIX shells, a backslash (\) has a special meaning so you may need to substitute a double backslash (\\). For example: ctxlpr -P "\\\\PRINTSRVR\\Sales_HP4000" mydoc.ps

If you are using a client device that uses direct printer port mapping:
ctxlpr -P lpt2 mydoc.ps
Printing from Applications

The exact configuration of how to set up printing from applications depends on the behavior and user interface of the UNIX application.

If the user interface for an application allows you to specify the actual printer command to use when printing, you can configure client printing by replacing the lpr or lp command with the ctxlpr command.

When a user connects to the server and prints from the application in a session, the server redirects the output to the mapped client printer.

Often, in this type of application, you can also specify the command-line modifiers on a different line. You can use the same switches for ctxlpr as when printing from the command line. For example, use -P with a printer name (or printer port) to print to a printer other than the default; -b for background printing, and so on.

Note: If the user interface of an application does not allow you to specify the actual printer command to use when printing, find out whether or not the application (or window manager) uses a configuration file where you can replace the lpr command functionality with ctxlpr.
Troubleshooting Printing

Because UNIX applications generally produce only UNIX ASCII text or PostScript output, PCL (Printer Control Language) printers are not suitable. Therefore, ensure your client printers support PostScript. If you do not have a PostScript printer, install a utility such as Ghostscript to convert PostScript files to a different output format, such as PCL.

If text does not print correctly, this may be due to carriage return / line feed differences between UNIX and DOS text files. To print a UNIX text file to a Windows printer, use a utility such as unix2dos. For example, to print a UNIX text file called "printfile" type:

On Solaris:

unix2dos printfile | ctxlpr

On HP-UX:

ux2dos printfile | ctxlpr

Alternatively, use Perl instead. For example, type:

perl -pe 's/
$/\r\n/' printfile | ctxlpr

Or, create a script file called "unix2dos" that includes the following:

```bash
#!/bin/sh
perl -pe 's/
$/\r\n/' "$@
```

Make the script file executable using chmod a+rx unix2dos. You can now use the script file just like the unix2dos utility.
Connecting to a Remote Server from an ICA Session

You can establish a connection to a remote server from within an ICA session.

When you establish a remote session, you must set the $DISPLAY environment variable in the remote session to ensure that graphics, keystrokes, and mouse clicks are sent back to your ICA session. To simplify the setting of $DISPLAY, use the $CITRIX_REMOTE_DISPLAY environment variable.

Example

The following example shows how to establish a connection to the remote server “Emily” from within an ICA connection to the server “Bagpuss” and how to correctly set the value of the $DISPLAY variable using $CITRIX_REMOTE_DISPLAY.
To connect to the remote server Emily from an ICA session

1. Establish an ICA connection to “Bagpuss”.

2. Open a terminal window and display the value of the $CITRIX_REMOTE_DISPLAY environment variable. At a command prompt, type:

   ```
   setenv | grep CITRIX_REMOTE
   ```

   The system displays a value; for example, bagpuss:10.0.

3. Make a note of the value of $CITRIX_REMOTE_DISPLAY.

4. Establish a remote logon session to “Emily” using the rlogin command:

   ```
   rlogin emily
   ```

5. Enter your logon password.

6. Open a terminal window and set the value of the $DISPLAY environment variable to the value of $CITRIX_REMOTE_DISPLAY. For example, if you are using a C shell, type:

   ```
   setenv DISPLAY bagpuss:10.0
   ```
These topics describe how to configure a XenApp for UNIX server to provide the required resource access and session behavior for the client users of your network and include information about:

- Configuring the server
- Screensaver recommendations
- Customizing the appearance of a server
- Configuring X server settings
You can configure your server in different ways to control access to services for users connecting to the server. The combination of settings you use depends on how you intend to use your servers. From the server, you can configure settings that include:

- The number of ICA sessions you want to allow at this server.
- What happens to a session if the connection is broken or times out.
- Whether or not to allow local printer mapping. If you enable printer mapping from the server, client users can configure and use their local printer to print from applications that are actually running on the server.
- Whether or not to allow local clipboard mapping. If you enable clipboard mapping from the server, client users can copy and paste text between applications running on the client device and the remote applications running on the server.
- Whether or not to allow shadowing.
- The maximum permitted session duration, and how long to leave idle or disconnected sessions before timing out.
- Whether or not to allow users to log on without a home directory.

**Note:** User access to commands and sessions is controlled by the ctxsecurity function.
Controlling Logon Settings

When client users connect to a server, the users need to supply a user name and password (unless they are accessing an application published for anonymous use). Users can either type this information in the dialog box that appears when they connect to the server or published application, or configure the plugin so that their user name and password are saved as part of the properties for a particular connection.

You can also use the ctxcfg tool on the server to configure settings that give you and client users flexibility and security when logging on.

To display the current logon settings

1. Log on to the server as an administrator.
2. At a command prompt, type:

   ctxcfg -a list

   This displays the current logon settings.

   ![Terminal window](image)

   Note: The list argument never displays passwords.
To change the logon settings

1. Log on to the server as an administrator.

2. At a command prompt:

<table>
<thead>
<tr>
<th>To</th>
<th>Use the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the server so that if logon details are set on the client device, they are used.</td>
<td>ctxcfg -a INHERIT</td>
</tr>
<tr>
<td>Configure the server so that a user logging on is always prompted for a password, regardless of any password set on the server or the client device.</td>
<td>ctxcfg -a prompt=TRUE</td>
</tr>
<tr>
<td>Configure the server so that a user logging on is not prompted for a password.</td>
<td>ctxcfg -a prompt=FALSE</td>
</tr>
<tr>
<td>Set a default user name for all users who log on to the server. For example, you can use this to set up a guest user account.</td>
<td>ctxcfg -a user=name</td>
</tr>
<tr>
<td>Set a password for all users who log on to the server. Type pass as a keyword; ctxcfg then displays a prompt where you can type the password. Note that if you did not set up a user name, this setting is ignored.</td>
<td>ctxcfg -a pass</td>
</tr>
<tr>
<td>Erase any user name and password details that were set (using the user and pass options) and configure the server to use logon details set on the client device.</td>
<td>ctxcfg -a ERASE</td>
</tr>
</tbody>
</table>

Displaying a Message of the Day

You can specify a message of the day to display to users as they log on. Text stored in /var/CTXSmf/motd appears in a message box before logon, up to a maximum size of 2 KB.

Configuring RSA SecurID Support

XenApp supports RSA SecurID Versions 4.2 and 5.0, allowing your users to log on to XenApp servers using RSA SecurID authentication.

Before you configure your servers for RSA SecurID support, ensure that you installed SecurID correctly. Citrix recommends that you test whether or not you can log on to your system using RSA SecurID before you attempt to use SecurID with XenApp.
To configure RSA SecurID Support on XenApp

1. Log on as root to the server.

2. Go to the directory where RSA SecurID is installed, and change to the prog directory below it.

3. Find the program files Xprompt (this file is called XPrompt in Version 4.2) and sdfindshell.

4. Copy the files into the /usr/sbin directory. Note that the copy of XPrompt must use this spelling, regardless of whether the original is spelled Xprompt or not.

5. Make the copy of XPrompt executable by using chmod +x.
Setting the Number of Permitted ICA Connections

You can specify a maximum number of concurrent ICA connections that a particular server will support.

**To check the current number of permitted connections**

1. Log on to the server as an administrator.
2. At a command prompt, type:
   ```
   ctxcfg -l list
   ```
   This command displays the number of logons permitted or displays UNLIMITED if no limit is set.

**To change the number of permitted connections**

1. Log on to the server as an administrator.
2. At a command prompt:

<table>
<thead>
<tr>
<th>To set</th>
<th>Use the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>A maximum, where num is the number of concurrent connections you want to allow.</td>
<td>ctxcfg -l max=num</td>
</tr>
<tr>
<td>No limit to the number of concurrent sessions you want to allow.</td>
<td>ctxcfg -l max=UNLIMITED</td>
</tr>
</tbody>
</table>

**Note:** The number of ICA connections that a server can support is also affected by Citrix Licensing—see *Getting Started with Citrix Licensing* for more information.
Disabling New Logons

You can prevent any new logons to a particular server, although users can still reconnect to disconnected sessions.

To disable new logons

1. Log on to the server as an administrator.
2. At a command prompt, type:
   
   ctxcfg -k nomorelogons=1

   Note that this setting is reset each time XenApp restarts.
Controlling Behavior for Disconnected or Broken Connections

To display the current configuration for broken and timed-out connections

1. Log on to the server as an administrator.
2. At a command prompt, type:

   `ctxcfg -c list`

To configure the settings for disconnected and broken connections

1. Log on to the server as an administrator.
2. At a command prompt:

<table>
<thead>
<tr>
<th>To configure the server so that</th>
<th>Use the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broken connections are immediately reset.</td>
<td><code>ctxcfg -c broken=reset</code></td>
</tr>
<tr>
<td>Broken connections are disconnected.</td>
<td><code>ctxcfg -c broken=disconnect</code></td>
</tr>
<tr>
<td>A user is automatically logged off from a broken connection.</td>
<td><code>ctxcfg -c broken=logoff</code></td>
</tr>
<tr>
<td>A user can connect to a disconnected session from any client device.</td>
<td><code>ctxcfg -c reconnect=any</code></td>
</tr>
<tr>
<td>A user can connect to a disconnected session only from the original terminal.</td>
<td><code>ctxcfg -c reconnect=original</code></td>
</tr>
</tbody>
</table>

You can configure the system so that disconnected sessions are reset or logged off automatically after a time-out interval, or continue until a user (or an administrator) resets...
the session. See Controlling Time-Out Behavior for details about how to set a time-out interval for disconnected sessions.
Enabling or Disabling Printing for Users

Client printer mapping allows client users to use printers that are available on the client device from applications running on a server.

Use the ctxcfg tool with the -p switch to enable or disable client printer mapping.

To check if client printing is currently enabled or disabled

1. Log on to the server as an administrator.
2. At a command prompt, type:
   
   ctxcfg -p list

To enable or disable client printing

1. Log on to the server as an administrator.
2. At a command prompt:

<table>
<thead>
<tr>
<th>To</th>
<th>Use the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable client printing.</td>
<td>ctxcfg -p enable</td>
</tr>
<tr>
<td>Disable client printing.</td>
<td>ctxcfg -p disable</td>
</tr>
</tbody>
</table>
Enabling or Disabling Clipboard Mapping

Users can copy text and graphics between server-based applications and applications running locally on the client device. Even if an application is running on the server, the clipboard behaves as if it is on the client device.

Use the ctxcfg tool with the -C switch to enable or disable client clipboard mapping.

To check if the client clipboard is currently enabled or disabled

1. Log on to the server as an administrator.
2. At a command prompt, type:
   
   ctxcfg -C list

To enable or disable the client clipboard

1. Log on to the server as an administrator.
2. At a command prompt:

<table>
<thead>
<tr>
<th>To</th>
<th>Use the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable client clipboard mapping.</td>
<td>ctxcfg -C enable</td>
</tr>
<tr>
<td>Disable client clipboard mapping.</td>
<td>ctxcfg -C disable</td>
</tr>
</tbody>
</table>
Providing Additional Graphics Clipboard Support

XenApp for UNIX provides users with the ctxgrab tool that lets them grab windows or screen areas and copy them from an application in an ICA session window to an application running on the local client device.

By default, ctxgrab is available to users connecting to published applications through the ctxwm window manager as follows:

- In a seamless window, right click the button in the top, left hand corner of the screen to display a menu and choose the Screen Grab option.
- In a “full screen” window, right click to display the ctxwm menu and choose the Screen Grab option.

Users connecting to a server desktop can run the tool by typing ctxgrab at a command prompt.

If you have users who require more extensive graphics clipboard support, you can deploy the ctxcapture tool. With ctxcapture users can:

- Grab dialog boxes or screen areas and copy them between an application in an ICA session window and an application running on the local client device, including non-ICCCM-compliant applications.
- Copy graphics between the client device and the X graphics manipulation utility XV. XV is a shareware utility that is available for download from the Internet.

Providing Users with xcapture

You do not have to do anything to make ctxcapture available to users connecting to a server desktop; it is available from a command prompt by typing ctxcapture.

To make ctxcapture available to users who are connecting to published applications, you make it available from the ctxwm window manager. To do this, you edit the ctxwmgrab.sh script to make ctxcapture, rather than ctxgrab, available.
To make ctxcapture available to users of published applications

1. Log on to the server as an administrator.

2. Open the ctxwmgrab.sh script.
   - On HP-UX and Solaris, this is located in the:
     /opt/CTXSmf/lib directory
   - On AIX, this is located in the:
     /usr/lpp/CTXSmf/lib directory

3. Find the following line:
   - On HP-UX and Solaris:
     
     exec /opt/CTXSmf/bin/ctxgrab
   - On AIX:
     
     exec /usr/lpp/CTXSmf/bin/ctxgrab

4. Substitute ctxgrab with ctxcapture.
Enabling or Disabling Shadowing

Session shadowing allows you to monitor the display of another active session. Shadowing lets you see what users are doing and interact with their sessions, using the keyboard and mouse. You can shadow active sessions on the same server.

Use the ctxcfg tool with the -s switch to configure shadowing.

**Note:** By default, any user can shadow any other session. To change this, amend your XenApp security settings.

**To display the current shadowing settings for the server**

1. Log on to the server as an administrator.
2. At a command prompt, type:
   ```bash
   ctxcfg -s list
   ```

   The shadowing configuration for the current server appears, for example:
To change the shadowing settings for the server

1. Log on to the server as an administrator.

2. At a command prompt:

<table>
<thead>
<tr>
<th>To enable shadowing</th>
<th>Use the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>So that sessions on the server can be shadowed. By default, input is set to on and notify to on.</td>
<td>ctxcfg -s enable</td>
</tr>
</tbody>
</table>

**To change the input and notify options**

<table>
<thead>
<tr>
<th>To enable shadowing</th>
<th>Use the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>So that the shadower can input keyboard and mouse actions to the shadowed session.</td>
<td>ctxcfg -s input=on</td>
</tr>
<tr>
<td>So that the shadower cannot input keyboard and mouse actions to the shadowed session.</td>
<td>ctxcfg -s input=off</td>
</tr>
<tr>
<td>So that the shadowed user gets a notification message requesting confirmation that the shadowing can occur.</td>
<td>ctxcfg -s notify=on</td>
</tr>
<tr>
<td>So that the shadowed user does not get a notification message.</td>
<td>ctxcfg -s notify=off</td>
</tr>
</tbody>
</table>

**To disable shadowing**

<table>
<thead>
<tr>
<th>To disable shadowing</th>
<th>Use the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>So that sessions on the server cannot be shadowed.</td>
<td>ctxcfg -s disable</td>
</tr>
</tbody>
</table>

**Important:** Disabling shadowing notification means that users might be shadowed by another user, but be unaware that they are being shadowed. Some countries require by law that users be notified before shadowing occurs.

**Example**

You may want to set up shadowing to help you solve technical support issues. The system administrator can show the user how to complete a task by shadowing the user’s session. To allow shadowing with notification and to allow the shadower to control the mouse and keyboard, use the command:

```
ctxcfg -s enable,input=on,notify=on
```
Controlling Time-Out Behavior

These settings specify time-out intervals in minutes or seconds. The time-outs are:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection</strong></td>
<td>The maximum connection duration (in minutes). If a connection duration is specified, the session is disconnected or terminated when the specified duration elapses. If NONE is specified, the connection timer is disabled.</td>
</tr>
<tr>
<td><strong>Disconnection</strong></td>
<td>The maximum duration that a disconnected session is retained (in minutes). If a disconnection duration is specified, sessions in the disconnected state are either terminated or logged off when the specified duration elapses. If NONE is specified, the disconnection timer is disabled.</td>
</tr>
<tr>
<td><strong>Log off</strong></td>
<td>Disconnected sessions can be logged off when the specified duration elapses. You must also set the disconnection time-out for this to take effect. If NONE is specified, the disconnected session is reset unless the disconnection time-out is also set to NONE. If log off fails, the session is reset.</td>
</tr>
<tr>
<td><strong>Idle</strong></td>
<td>The maximum idle time (time without user activity) allowed before the session is disconnected or reset (in minutes). If an idle duration is specified, the session is disconnected or reset when the specified interval elapses without any activity on the connection. If NONE is specified, the idle timer is disabled. To specify whether sessions are disconnected or reset, see To configure the settings for disconnected and broken connections. To specify an idle time-out period for anonymous users, see Configuring Anonymous Users.</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>The maximum duration that a session in the connected state exists on the server, prior to the user logging on or reconnecting (in minutes). When the specified duration elapses, the session is reset. This is useful, for example, if network problems result in sessions becoming stuck in the “conn” state; using this setting means you do not have to reset these sessions manually.</td>
</tr>
</tbody>
</table>
| **Client check** | The maximum period of time before the server checks that a client device is still connected and responsive (in seconds). If a client check time-out is set, the server sends a ping to unresponsive client devices when the specified interval elapses. If NONE is specified, the client check timer is disabled.  

**Note:** You must configure both client check and client response options if you want sessions to be disconnected automatically.
### To display the current time-out intervals

1. Log on to the server as an administrator.

2. At a command prompt, type:

   `ctxcfg -t list`

   The current time-out value for each setting appears. If a time-out interval is configured, the value is shown in minutes. If no time-out interval is configured, the keyword NONE shows that sessions will not be timed out.
To change the time-out intervals

1. Log on to the server as an administrator.

2. At a command prompt:

<table>
<thead>
<tr>
<th>To set</th>
<th>Use the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>A connection time-out (in minutes). All connections are terminated after this period.</td>
<td><code>ctxcfg -t connect=num</code></td>
</tr>
<tr>
<td>No connection time-out. All sessions continue until the user disconnects or logs off.</td>
<td><code>ctxcfg -t connect=NONE</code></td>
</tr>
<tr>
<td>A disconnection time-out (in minutes). Disconnected sessions are reset after this period unless you specified that they be logged off (see below).</td>
<td><code>ctxcfg -t disconnect=num</code></td>
</tr>
<tr>
<td>No disconnection time-out. Disconnected sessions remain until reset by a user or an administrator.</td>
<td><code>ctxcfg -t disconnect=NONE</code></td>
</tr>
<tr>
<td>A disconnection time-out (in minutes). Disconnected sessions are logged off after this period.</td>
<td><code>ctxcfg -t disclogoff=num</code></td>
</tr>
<tr>
<td>No logoff time-out. Disconnected sessions are reset unless the disconnect time-out was also set to None.</td>
<td><code>ctxcfg -t disclogoff=NONE</code></td>
</tr>
<tr>
<td>An idle time-out (in minutes). If no user activity is detected during this time, the connection is terminated.</td>
<td><code>ctxcfg -t idle=num</code></td>
</tr>
<tr>
<td>No idle time-out. All sessions continue until the user disconnects or logs off.</td>
<td><code>ctxcfg -t idle=NONE</code></td>
</tr>
<tr>
<td>An authentication time-out (in minutes). If a session remains in the connected state after this period, the session is reset.</td>
<td><code>ctxcfg -t authentication=num</code></td>
</tr>
<tr>
<td>No authentication time-out.</td>
<td><code>ctxcfg -t authentication=NONE</code></td>
</tr>
<tr>
<td>A client check time-out (in seconds). If the server receives no traffic from the client device during this period, it sends a ping to the client device to check if the plugin is still responding.</td>
<td><code>ctxcfg -t clientcheck=num</code></td>
</tr>
<tr>
<td>No client check time-out.</td>
<td><code>ctxcfg -t clientcheck=NONE</code></td>
</tr>
<tr>
<td>A client response time-out (in seconds). If the server does not receive a response to the ping sent to the client device during this period, the session is disconnected.</td>
<td><code>ctxcfg -t clientresponse=num</code></td>
</tr>
<tr>
<td>No client response time-out.</td>
<td><code>ctxcfg -t clientresponse=NONE</code></td>
</tr>
</tbody>
</table>
Controlling Time-Out Behavior

**Note:** Only new sessions are affected by changes to the time-out intervals. `ctxcfg -t` has no effect on anonymous users—to specify an idle time-out period for anonymous users, see *Configuring Anonymous Users*.

**Example**

If you expect users to dial in to the server, you may want to set the disconnect time-out to a suitable setting in case of a broken connection. Users can reconnect to their sessions during the time-out interval. To set the disconnection time-out to 15 minutes, type:

```
ctxcfg -t disconnect=15
```
Allowing Users to Log on without a Home Directory

By default, users whose home directories are unavailable cannot log on to the server. However, you can configure the server to allow users whose home directories are unavailable to log on. For example, you might do this if your users’ home directories are mounted on a network that is occasionally unreliable.

If you allow users whose home directories are unavailable to log on, all explicit users (that is, users who have their own user accounts) can log on, regardless of whether their home directories are available or not. Anonymous user accounts are not affected by these changes, because anonymous users are never allowed to log on without a home directory.

A temporary home directory is allocated to users in: /tmp/CTXSmf_uid where uid is a decimal number; for example, /tmp/CTXSmf_12345.

If users log on and their home directory is unavailable, the following message appears: “Your home directory is unavailable. Logging you in with temporary home directory: /tmp/CTXSmf_uid.”

**Important:** You must make your users aware that /tmp/CTXSmf_uid is temporary and may be deleted at a later stage. Any changes and additions that users make in this directory must be applied to their normal home directory when this becomes available.

In the unlikely event that there is a problem with the /tmp/CTXSmf_uid directory, the temporary home directory defaults to: / (the root directory). Note that some applications may not operate correctly when the home directory is / because users do not have write permissions.

To allow users whose home directories are unavailable to log on

1. Log on to the server as an administrator.
2. At a command prompt, type:

   ctxcfg -k lognohome=1
To prevent users from logging on without a home directory

1. Log on to the server as an administrator.

2. At a command prompt, type:

   `ctxcfg -k lognohome=0`
Configuring Mouse-Click Feedback for High Latency Connections

With mouse-click feedback, when a user clicks the mouse, the plugin software changes the mouse pointer to an hourglass to show that the user’s input is being processed. Mouse-click feedback is enabled by default.

Typically, you do not need to configure mouse-click feedback; however, for high latency connections, you may want to adjust this to improve your users’ interaction with the system.

You can configure the thresholds in which mouse-click feedback operates, or you can disable mouse-click feedback. To do this, you use the ctxcfg command with the -m option:

```
ctxcfg -m [enable | disable] [lower_threshold=num] [upper_threshold=num] [list]
```

About the Thresholds

Mouse-click feedback is controlled by upper and lower threshold values, which are like switches that determine when mouse-click feedback is on or off. The thresholds are the network delay between client device and server (that is, the latency) that triggers the display of the hourglass symbol.

- **Upper threshold.** If the latency exceeds the upper threshold, the hourglass symbol appears.

- **Lower threshold.** If the latency falls below the lower threshold, the hourglass symbol does not appear.

- **Between the two thresholds.** What happens between the upper and lower thresholds depends upon whether the latency is increasing or decreasing. If the latency was previously above the upper threshold but falls to between the two thresholds, the hourglass symbol appears until the latency drops below the lower threshold. If the latency was previously below the lower threshold but increases to between the two thresholds, the hourglass symbol does not appear until the latency increases above the upper threshold. This controls the sensitivity of mouse-click feedback, and prevents the hourglass from flickering on and off as the latency fluctuates.

By default, the upper threshold is 500 milliseconds and the lower threshold is 150 milliseconds. The following diagram illustrates what happens between the default threshold values.
Configuring Mouse-Click Feedback for High Latency Connections

Check using:

- `ctxcfg -D list`
- `ps -ef | grep ctxcdm`
- `ctxsec -c dm -l`
- `ctxmount /ctxmnt/Username/default`

Flowchart:

1. Is CDM enabled?
   - No: `ctxcfg -D enable, access={ro | rw}`
   - Yes: Is the CDM daemon running?
     - No: `ctxsrvc start cdm`
     - Yes: Is the user/group allowed to use CDM?
       - No: `ctxsec`
       - Yes: Is the drive available?
To change the mouse-click feedback thresholds

1. Log on to the server as an administrator.
2. At a command prompt, type:
   ```bash
   ctxcfg -m lowerthreshold=num,upperthreshold=num
   ```
   where `num` is the threshold value in milliseconds.

To disable mouse-click feedback

1. Log on to the server as an administrator.
2. At a command prompt, type:
   ```bash
   ctxcfg -m disable
   ```

To display current mouse-click feedback settings

1. Log on to the server as an administrator.
2. At a command prompt, type:
   ```bash
   ctxcfg -m list
   ```
   Information similar to the following appears:

   Mouse click feedback: enabled

   Lower threshold for mouse click feedback: 150

   Upper threshold for mouse click feedback: 500
Generating and Using Server Configuration Details

You can generate a list of the current ctxcfg settings for a particular server. If you send the output to a file, you can use the file in a shell script to replicate identical configuration settings on other servers. You can also use a file as a temporary backup of the current configuration, allowing you to experiment with other settings, but easily restore your original settings, if desired.

To display a list of the current ctxcfg settings

1. Log on to the server as an administrator.
2. At a command prompt, type:
   
   ctxcfg -g
   
   This generates a list of the current settings.

Creating a Shell Script of the Current Configuration

When you use the -g option with the ctxcfg command, the generated list contains the commands and settings for the current configuration using the ctxcfg command-line syntax. You can redirect the output of this command to a file and use the file as a shell script to restore (or set) this configuration.
To propagate the same configuration from one server to another

You can use the output from ctxcfg -g if you want to configure a number of servers in the same way.

1. Complete the configuration of the first server. Generate a list of the server configuration using the ctxcfg command and the -g option, piping the output of the command to a file. Note that ctxcfg -g does not generate the logon password, so you need to enter this manually.

2. Log on to the next server as an administrator and run the file as a shell script.

Tip: You can use the scp (secure copy) command to propagate the shell script on a remote server.
ICA connections running graphical screensavers can consume considerable server resources. Therefore, Citrix recommends that you switch screensavers off. In XenApp for UNIX, screensavers are switched off by default.

**To switch screensavers off**

Run the `xset` command with the `s` option and `off` parameter:

```
xset s off
```

To ensure published applications are run in sessions with the appropriate screensaver settings, Citrix recommends you publish a script file that runs the `xset s off` command and then the application.

**Note:** Although you can switch screensavers off by default, CDE may override this setting. To switch the screensaver off in CDE, choose the Screen option in the Style Manager and set Screen Blanker to off.

**To switch screensavers on**

Although it is best to switch screensavers off, if you prefer not to (for example, for security reasons), you can use the X server “prefer blanking” screensaver option. This causes the screen to go blank, rather than display a pattern, when the screensaver is activated.

To switch screensavers on, run the `xset` command with the `s` option and `blank` parameter:

```
xset s blank
```

For example, to make the screen go blank after one minute, use the commands:

```
xset s 60
xset s blank
```

**To display the current screensaver setting**

To display the current settings, run the `xset` command with the `q` option.

```
xset q
```
Customizing the Appearance of XenApp

You can customize XenApp to change the appearance of the XenApp Login screen and the window manager, and remove the X font server from the font path.

Your XenApp installation includes script files that you can customize. These scripts are located in the following directories:

On HP-UX and Solaris:

/opt/CTXSmf/lib and /opt/CTXSmf/slib

On AIX:

/usr/lpp/CTXSmf/lib and /usr/lpp/CTXSmf/slib

The script ctxXtw.sh runs when the X server starts, and includes X server configuration settings such as the font path and the X security policy. By default, the XenApp X server does not use a security policy (for the X security extension). It is disabled by the option -sp /dev/null in ctxXtw.sh. If you want to use a security policy, write the security policy (see the Xserver man page for details about how to do this) and then change this option in ctxXtw.sh to point to the policy file.

**Note:** Information about the switches in ctxXtw.sh is contained in a file called ctxXtw.sh.readme.

The script ctxsession.sh runs after a user logs on. You can use this script file to customize the local environment for user sessions, such as defining the default window manager, configuring scripts, or setting environment variables for users.
Customizing the Login Screen

You can change the appearance of the Login screen by substituting the Citrix logo frame for a graphic of your choice. The graphic you choose must be in .xpm (X pixmap) format.

The graphic used in the Login screen is located in:

On HP-UX and Solaris:

/opt/CTXSmf/data/C/LOGO.xpm

On AIX:

/usr/lpp/CTXmf/data/C/LOGO.xpm

The image that appears is limited to 120 x 200 pixels and 256 colors. If you use a larger graphic, only the 120 x 200 pixels in the center of the graphic appear. If you use a smaller graphic, the image displayed is centered in the frame.

To display a different logo on the Login screen

1. Log on to the server as an administrator.

2. Rename the current Citrix LOGO.xpm file; for example: old_LOGO.xpm

3. Rename your new graphic to LOGO.xpm and move this to the appropriate …/CTXSmf/data/C/ directory (see previous).

The new graphic appears on the Login screen
Changing the Window Manager

Using ctxsession.sh you can configure the system to load a window manager other than CDE. You can do this for every user who logs on to the server, or for a particular user.

You can change the window manager that XenApp loads for connections to server desktops and published applications running in “full screen” windows. By default, the ctxwm window manager is loaded for all connections to published applications.

To use a different window manager for every user

Use the following procedure to load a new window manager for every user who logs on to the server.

Note: The window manager is not loaded for any initial programs that a user set on the client device. To do this, use the To use a different window manager for a particular user procedure.

1. Log on to the server as an administrator.

2. Install the new window manager.

3. Open the ctxsession.sh script and locate the following line:

   : ${CDE_WM:="/usr/dt/bin/dtsession"}

4. Change this line to:

   : ${CDE_WM="/path/window_manager"}

   where path is the location of the new window manager and window_manager is the name of the new window manager.

To use a different window manager for a particular user

Use the following procedure to load a new window manager for a particular user each time the user logs on. The new window manager is also loaded for any initial programs that the user set on the client device.

1. Log on to the server as an administrator.

2. Install the new window manager.
3. Open the ctxsession.sh script and locate the following lines:

```bash
#if [ -f $HOME/.ctx.session.sh ] ; then
# . $HOME/.ctx.session.sh
#endif
```

4. Remove the `#` character from the start of each line, so that these lines are no longer commented out.

5. In the user’s home directory, create a file called .ctx.session.sh.

6. In the .ctx.session.sh file, add the new window manager’s bin directory to the path:

```bash
PATH=${PATH}:/path
```

where `path` is the location of the new window manager’s bin directory.

7. Add lines to load the new window manager and suppress the message that tells the user that the window manager is being loaded:

```bash
DESKTOP_WM="/path"
DESKTOP_MESSAGE=""
```

where `path` is the location of the new window manager’s start file.

8. Add lines to load the new window manager when an initial program is launched, and suppress the message that tells the user that the window manager is being loaded:

```bash
INITIAL_APPS_WM="/path"
INITIAL_APPS_MESSAGE=""
```

where `path` is the location of the new window manager’s start file.

**Example**

The following example shows the lines required in the user’s .ctx.session.sh file to start the kde window manager:

```bash
PATH=${PATH}:/usr/local/kde/bin
DESKTOP_WM="/usr/local/kde/bin/startkde"
DESKTOP_MESSAGE=""
INITIAL_APPS_WM="/usr/local/kde/bin/startkde"
INITIAL_APPS_MESSAGE=""
```
The result is that every time a user logs on, the system checks for the .ctx.session.sh file in the user's home directory. If it finds this file, the system runs it and the new window manager is loaded. If the file is not found, or the user connects to a published application, CDE is loaded.
Troubleshooting the ctxwm Window Manager

This topic describes problems that you or your users may experience when using the ctxwm window manager, and provides possible solutions for them.

**Preventing Published Application Windows being Placed Off-Screen**

To prevent windows for published applications being positioned off-screen, use the `DontPlaceOff` option in the `system.ctxwmrc` file.

In `/opt/CTXSmf/data/C/system.ctxwmrc`, uncomment the following line:

```
#DontPlaceOff # do not allow windows to be placed off screen, even
   # if the application asks for them to be
```

**Ignoring Modifier Map Entries**

The modifier map entries set for the ctxwm window manager may cause some applications to behave unexpectedly. For example, the behavior of lock keys such as CAPS LOCK may be unpredictable. To make ctxwm ignore some modifier map entries, use the `IgnoreModifier` option in the `system.ctxwmrc` file. The `IgnoreModifier` option takes the form:

```
IgnoreModifier { keyword }, where keyword can be one or more of the following, separated by spaces:
```

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Modifier Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>shift</td>
<td>shift modifier</td>
</tr>
<tr>
<td>lock</td>
<td>lock modifier</td>
</tr>
<tr>
<td>control</td>
<td>control modifier</td>
</tr>
<tr>
<td>m</td>
<td>mod1 modifier</td>
</tr>
<tr>
<td>m1</td>
<td>mod1 modifier</td>
</tr>
<tr>
<td>m2</td>
<td>mod2 modifier</td>
</tr>
<tr>
<td>m3</td>
<td>mod3 modifier</td>
</tr>
<tr>
<td>m4</td>
<td>mod4 modifier</td>
</tr>
<tr>
<td>m5</td>
<td>mod5 modifier</td>
</tr>
<tr>
<td>a1</td>
<td>mod1 modifier</td>
</tr>
</tbody>
</table>
Troubleshooting the ctxwm Window Manager

<table>
<thead>
<tr>
<th>a2</th>
<th>mod2 modifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>a3</td>
<td>mod3 modifier</td>
</tr>
<tr>
<td>a4</td>
<td>mod4 modifier</td>
</tr>
<tr>
<td>a5</td>
<td>mod5 modifier</td>
</tr>
</tbody>
</table>

For example, in /opt/CTXSmf/data/C/system.ctxwmrc, add lines such as the following:

```
IgnoreModifier { m3 m5 lock } # Ignore lock key modifiers (Num/Scroll/Caps)
```

**Note:** Different systems can have different modifiers mapped to different keys.

## Fixing Input Focus Problems

Applications that do not follow one of the ICCCM input focus models may behave unexpectedly on XenApp for UNIX because ctxwm adheres strictly to ICCCM. These applications may not set the appropriate X properties to allow the window manager to determine how to handle focus. To address this issue, use the ForceFocus option in the system.ctxwmrc file. This option permits more flexibility for non-ICCCM compliant applications.

Use the ForceFocus option to list either the WM_NAME or WM_CLASS (instance or class) to identify windows where the focus should be set. Use the xprop utility to determine these values for windows with focus issues. The best value to use depends on whether you are configuring an isolated window or a set of application windows. To fix the focus issue for a single window, use the WM_NAME property. To fix the focus issue for a set of windows, use the WM_CLASS property. For example, the third party application Slickedit does not follow ICCCM. Adding the “Slickedit” WM_CLASS value to /opt/CTXSmf/data/C/system.ctxwmrc as follows fixes the focus issue for all the Slickedit application windows:

```
ForceFocus {
    “Slickedit”
}
```
Changing the Font Path

By default, the font path contains the X font server. However, you can remove the X font server from the font path by editing the ctxsession.sh script.

For information about the X font server, and how to set it up, refer to the documentation provided with the X font server.

About Font Servers and Font Paths

An X Windows session can obtain the fonts that it requires locally or from a font server. A font server provides sessions with fonts and performs font conversion. Typically, a font server is used to deploy a set of fonts across a network; it is also useful for applications that have particular font requirements, such as TrueType fonts.

The path that a session takes to search for fonts is determined by the font path. The ctxXtw.sh script on the server, that runs when the X server starts, sets the default font path. The ctxsession.sh script, that runs after a user logs on, checks whether or not the font path contains the X font server. If the font path does not contain the X font server, ctxsession.sh adds it (provided the X font server is running).

**Important**: XenApp does not start the font server. Therefore, Citrix recommends that you enable the font server to start automatically.

Removing the Font Server from the Font Path

You can remove the font server from the font path by editing the ctxsession.sh script.

For example, you may want to remove the font server from the font path if the font server causes performance problems on the XenApp server. Note, however, that performance problems are unlikely to occur unless many short-term applications run on the server and make demands on the font server.
To remove the font server from the font path

1. Log on to the server as an administrator.

2. Open the ctxsession.sh script and locate the following line:

   USE_FONT_SERVER=1

3. Set the USE_FONT_SERVER flag to zero:

   USE_FONT_SERVER=0
Configuring X Server Settings

To configure X server settings, such as switching on the backing store feature, you edit ctxXtw.sh which is a script file that runs when the X server starts. You can also edit ctxXtw.sh to configure settings for particular fixes to take effect. For more information, see the ctxXtw.sh.readme file.
Configuring Backing Store

You can switch on the backing store feature in the X server for applications that rely on this functionality. Backing store caches the contents of the window displayed by an application and, where necessary, automatically repaints the window from the cache.

By default, backing store is switched off.

When Should Backing Store be Switched On?

Only some applications require backing store to be switched on. An application may require backing store if the application appears to be running very slowly or users experience screen corruption problems.

Because the use of backing store can increase the bandwidth between the server and the client device, Citrix recommends that you do not switch backing store on unless you are deploying applications that require it.

To switch backing store on

1. Log on to the server as an administrator.
2. Open the ctxXtw.sh script and locate the following line:

   XTW_OPTS="-session $CITRIX_SESSION_ID -terminate -bs"

3. Delete the -bs parameter from this line to turn backing store on.

To switch backing store off

1. To switch backing store off, reinstate the -bs parameter in the ctxXtw.sh script.
Interactive Performance Tuning

XenApp lets you control the display of graphics in ICA sessions by allowing you to specify the length of delay for the buffering of graphics. You can do this by setting two parameters. Both set a delay time in milliseconds. Recommended settings are between 5ms and 100ms. Setting the delay time to a lower value makes the session more responsive to graphics updates, but may increase the bandwidth requirements for the connection.

To control the outbuffer delay time

1. Log on to the server as an administrator.

2. At a command prompt:

<table>
<thead>
<tr>
<th>To</th>
<th>Use the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the delay time, where num is the time in milliseconds</td>
<td>ctxcfg -o set=num</td>
</tr>
<tr>
<td>List the current setting</td>
<td>ctxcfg -o list</td>
</tr>
<tr>
<td>To reset the current setting to 100ms</td>
<td>ctxcfg -o reset</td>
</tr>
</tbody>
</table>

To control the buffer delay for Thinwire 2 graphics operations

1. Log on to the server as an administrator.

2. Open the ctxXtw.sh script and find the line that begins with

   XTW_OPTS

3. Add the command-line option -qandtdelay n; for example,

   XTW_OPTS="-session $CITRIX_SESSION_ID -terminate -qandtdelay 10 -bs"
Configuration Required for Fixes to Take Effect

This topic explains how to configure your server for particular fixes to take effect. If you do not require these fixes, you can disregard this topic.
Fixing the Disappearing Text Cursor Problem

To fix the disappearing text cursor problem, include the -notransfills switch in ctxXtw.sh. This switch turns off the transparent fills optimization setting that can cause this problem with some plugins and 256-color sessions.

In ctxXtw.sh, find the line that begins with XTW_OPTS and add -notransfills. For example:

```bash
XTW_OPTS="-session $CITRIX_SESSION_ID -terminate -notransfills -bs"
```
Enabling the Left-Hand Keypad of SPARC Keyboards

If you are using the CDE window manager, you need to configure your server to enable the left-hand keypad of SPARC keyboards. To do this, you include the bindings file, edit the xmbind.alias file, and edit users’ logon scripts, as follows:

To enable the left-hand keypad of SPARC keyboards

1. Copy the bindings file, included on the XenApp installation media or in the download, to the /usr/dt/lib/bindings directory. The bindings file contains keyboard mapping information.

2. Edit the /usr/dt/lib/bindings/xmbind.alias file. This file contains server and bindings file mapping information. Include the following line in the list of mappings:

   "Citrix Systems Inc"  citrix

3. To activate the Find key on the SPARC keypad, you must edit your users’ logon scripts, as follows:

   If you are using a C shell, add the command:

   xmodmap -e "keysym F19 = SunFind" >& /dev/null

   If you are using a Bourne shell, add the command:

   xmodmap -e "keysym F19 = SunFind" 1>/dev/null 2>&1

Note: For this fix to take effect, you must also ensure that your users are running Version 6 (or later) plugins.
Fixing the Disappearing X Cursor Problem

In applications, such as Sunguard Forex, that hide the X cursor and use their own bitmap cursor, problems with the X cursor can occur over high-latency connections. To fix the disappearing X cursor problem, include the -notranscursor switch in ctxXtw.sh. This switch stops the application from causing the X cursor to disappear.

In ctxXtw.sh, find the line that begins with XTW_OPTS and add -notranscursor. For example:

```bash
XTW_OPTS="-session $CITRIX_SESSION_ID -terminate -notranscursor -bs"
```
Fixing Screen Refresh Problems

If an application has a complex graphical interface and you encounter screen refresh problems, include the -frameexpose switch in ctxXtw.sh. This switch forces the server to redraw the application from the server’s frame buffer. With complex screen displays, this method is faster than allowing the application to redraw itself.

In ctxXtw.sh, find the line that begins with XTW_OPTS and add -frameexpose. For example:

XTW_OPTS="-session $CITRIX_SESSION_ID -terminate -frameexpose -bs"

Cadence Applications

For Cadence applications, you must also include the -palette and -noredrawpalette switches because Cadence uses palette animation that sends one palette change per second. Use the -palette switch to filter out these unnecessary palette changes. Other palette changes are sent to the client device, but only after a delay of 1500 milliseconds (1.5 seconds). The -noredrawpalette switch reduces the communication between the server and the client device, if the application changes colors that are not currently visible in the session.

Note: A possible side-effect of including the -palette switch is that the sending of palette changes from server to client device is delayed. This means that it can take longer for objects to appear properly and, at first, objects may appear in unexpected colors until the new palette is sent. For example, you may see this effect when a splash screen first appears or when CDE first appears. This is normal.

XTW_OPTS="-session $CITRIX_SESSION_ID -terminate -frameexpose
-palette 1500 -noredrawpalette"

If this setting does not improve performance sufficiently, use -palette 3500 instead:

XTW_OPTS="-session $CITRIX_SESSION_ID -terminate -frameexpose
-palette 3500 -noredrawpalette"

Tip: You may also find it beneficial to switch on backing store.
Fixing NUM LOCK Problems

Some applications may behave unexpectedly when NUM LOCK is in the modifier map. By default, the NUM LOCK modifier map entry is enabled. To disable it, include the -nonumlockmodmap switch in ctxXtw.sh.

In ctxXtw.sh, find the line that begins with XTW_OPTS and add -nonumlockmodmap. For example:

```
XTW_OPTS="-session $CITRIX_SESSION_ID -terminate -nonumlockmodmap -bs"
```
Fixing Java Application Splash Screen Problems

If a user clicks on a splash screen displayed by a Java application, the splash screen may hang or the application may start slowly. This is caused by the Java application and the window manager repeatedly setting the input focus of the X server. You can address this issue by reducing the CPU usage. To do this, include the -ipfocussleepinterval switch in ctxXtw.sh and set it to the length of time in microseconds that the X server should sleep. You can set this value to between zero and 1000 microseconds. Normally 100 microseconds is sufficient, but you may need to experiment to determine the best value.

In ctxXtw.sh, find the line that begins with XTW_OPTS and add -ipfocussleepinterval. For example:

```
XTW_OPTS="-session $CITRIX_SESSION_ID -terminate
-ipfocussleepinterval 100 -bs"
```
Disabling Color Cursor Support

XenApp supports color cursors by default. Color cursors can be any two colors of your choice. To disable this feature, include the -nocolorcursors switch in ctxXtw.sh.

In ctxXtw.sh, find the line that begins with XTW_OPTS and add -nocolorcursors. For example:

```
XTW_OPTS="-session $CITRIX_SESSION_ID -terminate -nocolorcursors -bs"
```
Disabling Scrollmouse Support

You can turn off the X server’s capability to handle any scrollmouse events sent from the client device by including the -noscrollmouse switch in ctxXtw.sh.

In ctxXtw.sh, find the line that begins with XTW_OPTS and add -noscrollmouse. For example:

```
XTW_OPTS="-session $CITRIX_SESSION_ID -terminate -noscrollmouse -bs"
```
Color Depth Limitations

The limitations relating to color depth depend on the types of applications to which users connect.

Applications Requiring Writable Palettes

Some X applications require writable palettes, known as PseudoColor visuals, for color or image manipulation. However, XenApp supports only writable palettes in ICA sessions using a color depth of 256 colors. Therefore, applications requiring PseudoColor visuals will not work in ICA sessions using High Color and True Color color depths. This is because High Color and True Color sessions use TrueColor visuals, in which colors are predefined and cannot be changed.

If users connect to applications that require PseudoColor visuals, ensure that the ICA connection uses a color depth of 256 colors. If a connection is made at a higher color depth, the application may display an error message. To check if an application requires PseudoColor visuals, refer to the application’s documentation, or test the application on the server console or in a published desktop to ensure that it works.

To configure an application to use a color depth of 256 colors when connecting using the Web Interface, use the ctxappcfg tool with the Color Depth option.

Applications Requiring 16-bit High Color

XenApp supports 15-bit High Color connections, although some plugins refer to High Color as 16-bit in the Window Color property settings.

Some applications explicitly require a 16-bit display and will, therefore, not run in a 15-bit High Color connection. Other applications that require a 16-bit display may attempt to run in a 15-bit connection and fail, causing screen corruption. If you require a high color resolution to run these applications, use a True Color (24-bit) connection instead.
Multimonitor Display Limitations

The limitations of multimonitor display depend upon whether users connect to applications running in multimonitor mode using seamless or remote desktop windows.

Limitations Using Seamless Windows

If you use a seamless window, the primary monitor must be the left-most and top-most monitor. If you attempt to use a seamless window in multimonitor mode with another configuration, the ICA session reverts to running a full-screen window that spans the virtual desktop.

The color depth of an ICA session is limited by the lowest color depth in the display. For example, on a dual-monitor system, if one graphics card is configured to display 256 colors and the other graphics card is configured to display 24-bit color, the ICA session color depth is limited to 256 colors, regardless of the monitor on which the session appears.

If you are using graphics card drivers that create a virtual desktop, ICA sessions are maximized to fill the virtual desktop.

Pop-up message boxes, dialog boxes, and windows displayed by applications running in a seamless window may appear centered relative to the center of the entire desktop. When using graphics card drivers that create a virtual desktop, these elements are centered relative to the center of the virtual desktop.

Limitations Using Remote Desktop Windows

If you use a remote desktop window, pop-up message boxes, dialog boxes, and windows appear centered in the session window, regardless of how the ICA session window appears across multiple monitors.
Advanced Topics

These topics describe advanced system administration and include information about the following:

- Configuring anonymous user settings
- Configuring XenApp security
- Understanding and configuring the ICA Browser Service
- Load balancing published applications
- Configuring ICA gateways
- Using ICA with network firewalls
- Configuring the TCP/IP port number
- Configuring session status logging
- Configuring the operating system for a large number of connections
- Configuring non-English language support
Configuring Anonymous Users

During installation, you can create a special user group called ctxanon on the server, together with 15 local anonymous user accounts. These accounts allow 15 users guest access to applications that you publish for anonymous use.

Anonymous user accounts do not usually require further maintenance; however, their properties can be displayed and modified using the ctxanoncfg command.

**Note:** You must be root to display and update anonymous user settings.
Displaying Anonymous User Settings

Use ctxanoncfg to display the current number of anonymous user accounts, the naming of the accounts, the anonymous user group name, and the idle time-out period.

To display anonymous user settings

1. Log on to the server as the root user.

2. At a command prompt, run ctxanoncfg with the -l option to display anonymous user settings:

   ```
   ctxanoncfg -l
   ```

   ```
   $ ctxanoncfg -l
   Anonymous group ctxanon
   Anonymous user anon1
   Anonymous user anon2
   Anonymous user anon3
   Anonymous user anon4
   Anonymous user anon5
   Anonymous user anon6
   Anonymous user anon7
   Anonymous user anon8
   Anonymous user anon9
   Anonymous user anon10
   Anonymous user anon11
   Anonymous user anon12
   Anonymous user anon13
   Anonymous user anon14
   Anonymous user anon15
   Anonymous session idle timeout is 10 minutes
   $
   ```
Configuring Anonymous User Settings

You can use ctxanoncfg to change the number of anonymous user accounts, the names of the anonymous user accounts, and the idle time-out period for anonymous user sessions. You can also use ctxanoncfg to specify a particular shell or assign user ids to anonymous user accounts.

Tip: The ctxanoncfg command displays what it is doing at each stage, together with any errors that may occur. To suppress the display of this information, use the -q (quiet) option with the ctxanoncfg command. For example, type: ctxanoncfg -n 20 -q
Changing the Number of Anonymous Users

Use ctxanoncfg with the -n option to change the number of anonymous user accounts. You can create any number of anonymous user accounts, but the number you can use simultaneously is limited by your licensed user count.

Further options are available that allow you to change the naming of anonymous user accounts and the idle time-out period.

**Important:** You must stop XenApp on the server before you create anonymous users. If XenApp is running, use the ctxshutdown command to stop it.

To create anonymous users

1. Ensure XenApp is not running on the server and log on as root.

2. At a command prompt, use ctxanoncfg with the -n option to specify the new number of anonymous user accounts you require:

   ```
   ctxanoncfg -n number
   ```

   where `number` is the new number of anonymous user accounts.


Examples

To specify 20 anonymous user accounts, type:

```
ctxanoncfg -n 20
```

To delete all anonymous user accounts, type:

```
ctxanoncfg -n 0
```
Changing the Naming of Anonymous User Accounts

Use ctxanoncfg with the -b option to change how anonymous user accounts are named. By default, the ctxanon group contains 15 user accounts with names in the format anonx, where x is a number from one to 15. User account names can have a maximum of eight characters.

**Note:** You can use the -b option only when creating new anonymous user accounts; -b cannot be used to change existing anonymous user accounts.

**To change how anonymous user accounts are named**

1. After stopping XenApp, log on as root.

2. At a command prompt, type:

   ```
   ctxanoncfg -n number -b name
   ```

   where **number** is the new number of anonymous user accounts, and **name** is the new name of the accounts.

**Example**

To create 25 anonymous user accounts called “guest1,” “guest2” … up to “guest 25,” type:

```
ctxanoncfg -n 25 -b guest
```
Setting an Idle Time-Out Period

Use ctxanoncfg with the -t option to specify the idle time-out period, in minutes, for anonymous user sessions.

If there is no user activity within this time, a warning message informs users that they will be logged off after five minutes, unless they resume use of the session. The default idle time-out period is 10 minutes.

To specify an idle time-out period

1. After stopping XenApp, log on as root.
2. At a command prompt, type:

   ctxanoncfg -n number -t minutes

   where number is the new number of anonymous user accounts and minutes is the idle time-out period.

Examples

To create 25 anonymous user accounts with a time-out period of 30 minutes, type:

ctxanoncfg -n 25 -t 30

To alter only the time-out period to 20 minutes, type:

ctxanoncfg -t 20
Specifying a Particular Shell for Anonymous Users

When anonymous user accounts are created, the default system shell is assigned to these accounts; for example: /bin/sh. However, you can specify a particular shell to use for anonymous user accounts, using ctxanoncfg with the -s option.

To specify a particular shell

1. After stopping XenApp, log on as root.
2. At a command prompt, type:

   ctxanoncfg -n number -s shell

   where number is the new number of anonymous user accounts and shell is the shell you want to assign to these accounts.

Example

To create 25 anonymous user accounts that use the C shell, type:

   ctxanoncfg -n 25 -s /bin/csh
When anonymous user accounts are created, XenApp automatically assigns available user ids to these accounts. However, you can assign specific user ids to anonymous user accounts. To do this, you use ctxanoncfg with the -u option and specify the first user id in the range.

**To assign specific user ids**

1. After stopping XenApp, log on as root.
2. At a command prompt, type:

   ```bash
ctxnanoncfg -n number -u uid-number
   ``

   where *number* is the new number of anonymous user accounts and *uid-number* is the first user id you want to generate.

**Example**

To create 10 anonymous user accounts with user ids 10,027 to 10,036, type:

```
ctxnanoncfg -n 10 -u 10027
```
Troubleshooting Anonymous User Accounts

If you experience problems with anonymous user accounts, delete the current anonymous user configuration, using ctxanoncfg with the -clear option, and then create new anonymous user accounts. The -clear option removes all internal anonymous user account configuration, such as the home directories and entries in the password file.

To delete all anonymous user account configuration

1. After stopping XenApp, log on as root.

2. At a command prompt, type:

    ctxanoncfg -clear

Anonymous User Accounts and NIS Domains

All anonymous user accounts are created as local (non-NIS) accounts, with home directories in /usr/anon. Citrix recommends that you do not attempt to reconfigure these accounts to be NIS accounts, or move the home directories for these users onto non-local (for example, NFS) file systems.

To create user home directories on another file system, create a symbolic link from /usr/anon to the desired file system.
When you install XenApp, default security settings automatically control user access to various commands. By default, users can log on, send messages, and shadow other sessions, but they are denied access to all other commands.

XenApp security lets you tighten or relax user access to commands and sessions. With XenApp security you can:

- Change the default security settings. For example, by default, all users can shadow other users’ sessions, but you may want to prevent this.
- Provide groups of users with access to commands and sessions. For example, you may want to give the “helpdesk” user group the rights to connect, disconnect, and reset other users’ sessions.
- Deal with exceptions on an individual user basis. For example, you may want to prevent a particular user from being able to send messages to other users’ sessions.
Security Overview

Which Users Are Affected by Security?

XenApp security controls user access to specific commands and sessions.

However, security does not control administrator access to commands and sessions. This means the ctxadm group is unaffected by XenApp security. Security controls the access rights of the root user and ordinary users (explicit and anonymous users).

Who Can Do What in XenApp

The following table provides a brief summary of which users can do what in XenApp. Only the functions indicated by “ctxsecurity” are controlled using security.

<table>
<thead>
<tr>
<th>Functions/commands</th>
<th>root user</th>
<th>ctxadm</th>
<th>Other users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install and remove XenApp</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Start and stop server processes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Configure the server</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Log on to the server</td>
<td>ctxsecurity</td>
<td>Yes</td>
<td>ctxsecurity</td>
</tr>
<tr>
<td>Query who is on the server</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Perform actions on others’ sessions,</td>
<td>ctxsecurity</td>
<td>Yes</td>
<td>ctxsecurity</td>
</tr>
<tr>
<td>such as shadowing or resetting sessions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perform actions on their own sessions</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Send messages</td>
<td>ctxsecurity</td>
<td>Yes</td>
<td>ctxsecurity</td>
</tr>
</tbody>
</table>

Note: If root is unable to log on at the server, this may be due to the CONSOLE setting in the /etc/default/login file (the /etc/security/user file on AIX), that can be used to prevent root logging on at a terminal other than the one specified. The ctxsecurity command cannot be used to override the CONSOLE setting.

Which Functions Can ctxsecurity Control?

XenApp security controls access to specific functions called secured functions. The secured functions are shown in the following table:

<table>
<thead>
<tr>
<th>Secured function</th>
<th>Security determines…</th>
</tr>
</thead>
<tbody>
<tr>
<td>login</td>
<td>Which users can log on to the XenApp server.</td>
</tr>
<tr>
<td>sendmsg</td>
<td>Which users can use ctxmsg to send messages to other users’ sessions.</td>
</tr>
<tr>
<td>connect</td>
<td>Which users can use ctxconnect to connect to other users’ sessions.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>disconnect</td>
<td>Which users can use ctxdisconnect to disconnect other users’ sessions.</td>
</tr>
<tr>
<td>logoff</td>
<td>Which users can use ctxlogoff to log off other users’ sessions.</td>
</tr>
<tr>
<td>reset</td>
<td>Which users can use ctxreset to reset other users’ sessions.</td>
</tr>
<tr>
<td>shadow</td>
<td>Which users can use ctxshadow to shadow other users’ sessions.</td>
</tr>
<tr>
<td>cdm</td>
<td>Which users can use client drive mapping to access their local drives.</td>
</tr>
</tbody>
</table>

**Controlling Security at Different Levels**

Security can be controlled at the:

- User level—that is, UNIX user level
- Group level—that is, UNIX group level
- Global level—that is, UNIX global level

A global security setting exists for every secured function. When you install XenApp, security is automatically controlled at the global level for each secured function. For example, by default, all users can send messages to other sessions.

However, you can also configure security for individual users or for groups of users. For example:

- If you want to prevent a user from sending messages to other sessions, you can set up user-level security to deny access to ctxmsg.
- You can set up group-level security for the Support group to allow members of this group to reset other users’ sessions using ctxreset.

If no user or group-level security exists, the global security level determines user access rights.

**The Security Checking Process**

To configure XenApp security or troubleshoot security, you need to understand how the security checking process works.

When a user attempts to run a secured function, XenApp checks whether or not the user has the rights to do so. It first checks the user security level, then, depending on the result, the group security level. If neither user nor group-level security exists, a final check is made at global security level.

The following diagram shows each step in the security checking process, using the example of a user attempting to run the ctxshadow command:
Security Overview

Does user-level security exist for this user?

Yes

Is shadowing allowed?

Yes

Allow shadowing

No

Deny shadowing

No

Does the user belong to a group where group-level security exists?

Yes

Does at least one group allow shadowing?

Yes

Allow shadowing

No

Deny shadowing

No

Does the global security level allow shadowing?

Yes

Allow shadowing

No

Deny shadowing
Default Security Settings

A global security setting always exists for each secured function. The global setting acts as the default, when neither user level nor group level security exists. Because the primary function of security is to deny access to unauthorized users, the global security setting can be thought of as the last line of defense.

After installation, the default settings are:

<table>
<thead>
<tr>
<th>Secured function</th>
<th>Default global setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>Allow</td>
</tr>
<tr>
<td>Sendmsg (ctxmsg)</td>
<td>Allow Deny for anonymous users</td>
</tr>
<tr>
<td>Connect (ctxconnect)</td>
<td>Deny</td>
</tr>
<tr>
<td>Disconnect (ctxdisconnect)</td>
<td>Deny</td>
</tr>
<tr>
<td>Logoff (ctxlogoff)</td>
<td>Deny</td>
</tr>
<tr>
<td>Reset (ctxreset)</td>
<td>Deny</td>
</tr>
<tr>
<td>Shadow (ctxshadow)</td>
<td>Allow Deny for anonymous users</td>
</tr>
<tr>
<td>Cdm</td>
<td>Allow</td>
</tr>
</tbody>
</table>

**Note:** By default, root cannot log on to the server from a client device. However, if your super user has a different account name from “root” or multiple account names, the super user can log on from a client device.

To change the default settings, see Configuring Security Settings.
Displaying Security Settings for a Function

Use the -l (list) option with the ctxsecurity command to display security settings for a particular function. You must specify the secured function for which you want to display settings. All levels of security (user, group, and global) appear for the function.

To display security settings for a function

1. Log on to the server as an administrator.

2. At a command prompt, type:

   `ctxsecurity secured-function -l`

   where `secured-function` is one of: login, sendmsg, connect, disconnect, logoff, reset, shadow, or cdm.

Example

To display security settings for the ctxshadow function, type:

`ctxsecurity shadow -l`

Security settings such as the following appear:

```
global allow
group users deny
```
Configuring Security Settings

You can use the ctxsecurity command to change the global security settings or to configure user and group level security.
To change a global security setting

You can use the ctxsecurity command with the -a (all) option to change the global security setting for a secured function.

1. Log on to the server as an administrator.

2. At a command prompt, type:

   `ctxsecurity secured-function -a allow|deny`

   where `secured-function` is one of: login, sendmsg, connect, disconnect, logoff, reset, shadow, or cdm.

Example

To change the global security setting for the ctxshadow tool to deny, type:

`ctxsecurity shadow -a deny`
To configure security for a user

You can use the ctxsecurity command with the -u (user) option to configure security at the user level. For example, you might want to allow a particular user access to a function that is denied at the global level.

1. Log on to the server as an administrator.

2. At a command prompt, type:

   ctxsecurity secured-function -u user-name allow|deny

   where secured-function is one of: login, sendmsg, connect, disconnect, logoff, reset, shadow, or cdm.

Example

To allow the user “fred” to use the ctxreset command to reset other users’ sessions, type:

   ctxsecurity reset -u fred allow
To configure security for a group of users

You can use the ctxsecurity command with the -g (group) option to configure security at the group level. For example, you might want to allow a group of users access to a function that is denied at the global level.

1. Log on to the server as an administrator.

2. At a command prompt, type:

   `ctxsecurity secured-function -g group-name allow|deny`

   where `secured-function` is one of: login, sendmsg, connect, disconnect, logoff, reset, shadow, or cdm.

**Example**

To allow the group Support to use the ctxreset command to reset other users’ sessions, type:

`ctxsecurity reset -g support allow`
To inherit a security setting

You can use the inherit option with the ctxsecurity command to remove previously set security settings. This option is useful when you want to remove settings that are exceptional cases.

For example, the Management group is allowed to shadow other sessions, but the user Fred, a member of this group, is an exception and has been denied access to shadowing. When it is later decided to allow Fred to shadow, the administrator can use inherit to reinstate the group’s security setting. In effect, inherit removes Fred’s user-level security setting, and picks up the security setting from group level.

Users can inherit settings from the group or global level, while a group can inherit settings from the global level. Global security settings cannot inherit values.

1. Log on to the server as an administrator.

2. At a command prompt, type:

   `ctxsecurity secured-function { -u user-name | -g group-name } inherit`

   where `secured-function` is one of: login, sendmsg, connect, disconnect, logoff, reset, shadow, or cdm.

**Example**

To remove Fred’s user-level security setting for the ctxshadow command and reinstate the group’s security setting, type:

```
ctxsecurity shadow -u fred inherit
```

The result is that Fred inherits a security setting. XenApp checks which groups Fred belongs to, and whether any of these groups have a group level security setting. If at least one group level setting exists that allows shadowing, Fred inherits the right to shadow. Otherwise, if at least one group level setting exists that denies shadowing, Fred is not permitted to shadow. If no group level setting exists, Fred inherits rights from the global level.
In the following examples, security is tightened and then used to provide a group of users access to a particular function.

**Example 1: Locking Down Security**

After installation, the default security settings allow users to shadow other users’ sessions. However, the administrator decides to tighten security to prevent this.

The administrator does this by changing the global security setting for the shadowing function:

```bash
ctxsecurity shadow -a deny
```

**Exmaple 2: Giving Rights to a Group of Users**

Security is configured so that users are prevented from shadowing other users’ sessions. However, the “helpdesk” group needs to be able to shadow so they can help users with problems.

The administrator uses security to provide the “helpdesk” user group access to the shadowing function:

```bash
ctxsecurity shadow -g helpdesk allow
```
XenApp for UNIX and the ICA Browser Service

The ICA browser maintains data about published applications and XenApp servers. The ICA browser consists of a master browser, member browsers, and plugins. The ICA browser uses directed packets to communicate with other ICA Browser Services running on servers.

Citrix plugins query the browser service to obtain a list of published applications and XenApp servers. The plugin queries the browser service for the network address of servers and published applications when a session is launched.
Controlling the Master Browser

Every server runs the ICA Browser Service. One XenApp server is elected the master browser; all other XenApp servers on the network are member browsers. The master browser is a browser acting as a central information store. The master browser keeps track of the following information:

- The available servers
- The available published applications
- Performance and load information for servers

The master browser for each network is chosen by a master browser election. If the current master browser on a network is not responding, a new master browser election is held automatically. This provides high reliability for the browser service.

In general use, the browser service is invisible to you and does not affect the continued operation of XenApp. However, you may want to manipulate the possibility of a particular server becoming the master browser, because:

- Servers running different versions of XenApp provide different versions of the browser service when they are master browser. This can affect the features available to users. In particular, if you have servers running XenApp for Windows in your network, you may want to ensure that a server running XenApp for UNIX in the network does not become the master browser.

- The master browser service consumes more resources and may respond slowly if it is running on a heavily loaded server. Therefore, you may want to make sure that servers that receive many connections are less likely to become the master browser. If necessary, you can configure the settings of one or more dedicated servers in the network so that one of them is more likely to become the master browser.

To locate the master browser

You can use the ctxqserver command with the -master option to locate the server acting as the master browser.

1. Log on to the server as an administrator.

2. At a command prompt, type:

   `ctxqserver -master`

The address of the master browser on the local subnet appears. If no master browser is running, for example during a browser election, the error message “Error obtaining requested information” appears.
Manipulating Master Browser Elections

The browsers on a network subnet elect a master browser under any of the following conditions:

- The current master browser does not respond to another browser
- The current master browser does not respond to a plugin
- A XenApp server is started
- Two master browsers are detected on the same network subnet

A combination of factors affect the outcome of the election. The two main factors are:

- The version of XenApp running on the server
- The master browser preference setting for each server

You set this preference using the ctxbrcfg tool for XenApp for UNIX servers. Servers can be set to:

neutral The default value of “no preference” behavior in elections.

always Always attempt to become master browser.

never Never attempt to become master browser.

Other factors, such as the length of time a server has been running and whether the server is also a Windows NT domain controller (not applicable to XenApp for UNIX), can also affect an election result.

Tip: You can force a master browser election using the ctxqserver -election command.
Introducing any type of XenApp server into your network forces an election.

- The default master browser preference setting for a XenApp for UNIX server is neutral; that is, unbiased. If you add a server with this default setting to a network that includes XenApp for Windows servers in mixed mode that are also configured as unbiased in elections, the XenApp for UNIX server will not become the master browser. Under these circumstances, a XenApp for Windows server in mixed mode automatically has preference to become the master browser.

- If you add a XenApp for UNIX server to a network that includes only other such servers, it may become master browser if all the other servers are set to neutral.

**Important:** It is the combination of settings for all servers on the network that decides the results of an election. A XenApp for UNIX server could still win a master browser election with a XenApp for Windows server if the master browser preference on the Windows server is set to never.
Biasing the Results of Elections

If you do not mind which server becomes master browser

1. Leave the master browser preference setting on each server to the default setting of neutral or no preference, as appropriate for the type of server.

If you want a particular server to be the master browser

1. Configure the master browser preference on the server you want to become master browser to be always. Use the ctxbrcfg command for XenApp for UNIX servers. For XenApp for Windows servers, see the Citrix XenApp Administrator’s Guide.

2. Leave the master browser preference on the other servers to be neutral or no preference, as appropriate for the type of server. Do not set the other servers to be never—reserve this setting for a particular server that should never become master browser.

The changes you make using ctxbrcfg will cause a master browser election to occur. Wait a few moments for the election to take place and then check the master browser status using the ctxmaster command.

If you want to stop a particular server from becoming the master browser

1. Configure the master browser preference on the server that you do not want as the master browser to be never, using the ctxbrcfg command.

   **Important:** Do not set the master browser preference on all servers in a network to be never because unpredictable election results will occur.

2. Leave the master browser preference on the other servers that can become the master browser to be neutral or no preference as appropriate for the type of server. Any changes you make using the ctxbrcfg command will cause a master browser election to occur.

   **Note:** If the XenApp for UNIX server has more than one network interface card and is connected on more than one subnet, restrict the server to one subnet; for details, see If a Server Uses Multiple Network Interface Cards.
Configuring the ICA Browser

The ICA browser maintains data about published applications and XenApp servers. You can display and change the browser settings on a server using the ctxbrcfg tool. Any changes you make using ctxbrcfg will cause a master browser election to take place.

To control how the ICA browser behaves during browser elections

1. Log on to the server as an administrator.

2. At a command prompt:

<table>
<thead>
<tr>
<th>To</th>
<th>Use the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the server so that it always attempts to become the master browser in an election, subject to the presence and actions of other browsers.</td>
<td>ctxbrcfg -m always</td>
</tr>
<tr>
<td>Configure the server so that it refrains from participating in an election. Note that the server can still become the master browser under some circumstances.</td>
<td>ctxbrcfg -m never</td>
</tr>
<tr>
<td>Configure the default behavior of “no preference.”</td>
<td>ctxbrcfg -m neutral</td>
</tr>
</tbody>
</table>

The refresh period controls how often the browser on this server updates the master browser. The browser updates the master browser after the specified amount of time elapses. A short refresh period makes the master browser data more accurate, but increases CPU and network load.

To view or change the refresh interval for the ICA Browser Service

1. Log on to the server as an administrator.

2. At a command prompt:

<table>
<thead>
<tr>
<th>To</th>
<th>Use the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the current refresh interval.</td>
<td>ctxbrcfg -r list</td>
</tr>
<tr>
<td>Set a period (in minutes) at which the local browser service will update the master browser.</td>
<td>ctxbrcfg -r set=num</td>
</tr>
</tbody>
</table>

Note: The default settings work for most installations. Change them only when you understand the implication of each setting.
Starting and Stopping the ICA Browser

You can start and stop the ICA browser process on a server, without having to stop and start all the XenApp processes, using the ctxsrv tool.

If you stop the browser on a server, users cannot connect to published applications on this server, although they will still be able to connect to the server desktop. If you stop the browser process on the master browser, a master browser election will occur among the other servers on the network.

To start or stop the ICA browser using ctxsrv

1. Log on to the server as an administrator.

2. At a command prompt, type:

   ctxsrv {start|stop} browser
If a Server Uses Multiple Network Interface Cards

If a XenApp server has more than one network interface card (NIC) and is connected on more than one subnet, problems may occur if this server attempts to become master browser on a subnet. If the server becomes master browser on one subnet, it may assume it is also master browser on another subnet that already has a master browser.

To prevent this from occurring, you must configure the server so that the browser communicates only with other browsers on a particular subnet or NIC. This means that you must bind the server to a particular subnet or NIC.

To do this, you use the ctxbrcfg command with the -b option.

**To restrict the ICA browser to a particular subnet or NIC**

1. Log on to the server as an administrator.
2. Stop the browser by typing:

   ```
   ctxsrv stop browser
   ```

3. At a command prompt, type:

   ```
   ctxbrcfg -b set=address
   ```

   where *address* is the IP address or subnet address you want to restrict the ICA browser to, in *aaa.bbb.ccc.ddd* format—for example, 10.20.123.123.

4. Restart the browser by typing:

   ```
   ctxsrv start browser
   ```
To remove a restriction on an ICA browser

1. Log on to the server as an administrator.
2. Stop the browser by typing:
   ```
   ctxsrv stop browser
   ```
3. At a command prompt, type:
   ```
   ctxbrcfg -b unset
   ```
4. Restart the browser by typing:
   ```
   ctxsrv start browser
   ```

To display current restrictions on an ICA browser

1. Log on to the server as an administrator.
2. At a command prompt, type:
   ```
   ctxbrcfg -b list
   ```
   If there are no restrictions, the message “No address specified, binding to all available adapters” appears.
   
   If there are restrictions, the message “Browser bound to adapter address aaa.bbb.ccc.ddd” appears (where aaa.bbb.ccc.ddd is the IP address or subnet address to which the ICA browser is restricted).

Troubleshooting Multiple Network Interface Cards

If you bind the server to a subnet, make sure that there is only one NIC on this subnet, or the browser will not start and an error will be written to the system log. Instead, bind to a specific NIC rather than the network.
This topic introduces load balancing and explains how to tune load balancing in your XenApp installation.

Load balancing determines which servers are least busy and can best run an application. The master browser keeps track of the load levels and the number of users connected on each server. When a published application or desktop is launched from a client device, the master browser selects which server will run the application or desktop session, based on server load. For more information about the master browser, see XenApp for UNIX and the ICA Browser Service.

Load balancing also offers increased availability. By configuring a pool of servers capable of running your users’ applications, you can easily bring servers off-line for maintenance or add more servers for increased performance without affecting application availability.

If you are deploying applications using the Web Interface, load balancing works in the normal way. The Web Interface contacts the XML Service, which in turn contacts the master browser. The master browser then distributes connections among the servers, taking load factors into account.
Load Balancing a Group of Servers

By default, XenApp automatically monitors the number of users connected to each server and sends new connections to the server that is least busy.

However, if a user already has a disconnected session on a server, the disconnected session is reconnected, regardless of how busy the server is.

To load balance a group of servers

1. Publish the application on each server.

2. Allow users to connect to the published application. Connections are distributed among all the servers on which the application is published.

   Note: Load balancing works by identifying the names of published applications. Therefore, make sure that the application you want to load balance over a group of servers is given the same name in ctxappcfg on each server.
Tuning Load Balancing

Different types of servers—for example, with different processor speeds or available memory—can accept a different number of connections before becoming busy. If you find that some servers become busier than others with evenly distributed connections, you can tune load balancing so that this is taken into account.

You can bias the distribution of connections to take into account the relative speed and power of a server. To do this, you use ctxcfg with the -k loadfactor option to adjust the load factor.

By default, each server has a load factor of 100. However, if you have a server that is more powerful relative to the other servers in the group, you can increase the load factor to ensure that this server receives more connections. Likewise, if you have a server that is less powerful, you can decrease the load factor to ensure that it receives fewer connections. The load factor can be any number between 1 and 10000.

To tune the load on each server

1. Stop the browser by typing:
   `ctxsrv stop browser`

2. At a command prompt, type:
   `ctxcfg -k loadfactor=num`
   where *num* is a load factor value between 1 and 10000.

3. Start the browser by typing:
   `ctxsrv start browser`

Alternatively, you can use ctxcfg with the -l option to control the number of connections permitted on each server.

Examples

Example 1

There are 10 servers in a server farm, each running XenApp for UNIX. One server has a higher than average processor than the others, and you estimate that it can handle 50% more load than the other servers.

On the more powerful server, allow 50% more load than on the other servers in the group. At a command prompt type:

`ctxsrv stop browser ctxcfg -k loadfactor=150 ctxsrv start browser`
Example 2

There are five servers in a server farm, each running XenApp for UNIX. One server has a lower than average processor, and you estimate that it can handle 25% less load than the others.

On the less powerful server, allow 25% less load than on the other servers in the group. At a command prompt type:

ctxsrv stop browser ctxcfg -k loadfactor=75 ctxsrv start browser

To tune the number of connections on each server

1. When a user experiences problems running a session, use the ctxqsession command to identify the server to which the user is connected.

2. Count the active number of sessions on the server that is causing the problem, and then limit the maximum number of users who can log on to the server using ctxcfg and the -l option.

3. Limit the maximum number of users who can log on, on the other servers, in a similar way. For best results, set a value on each server.

Example

A word-processing application is published on a number of servers. Occasionally, a server becomes overloaded. This is due to a high number of users concurrently using the application (rather than that the application places a high demand on server resources, such as in the case of a CAD application). Therefore, you decide to limit the number of connections permitted on each server to 200.

On each server on which the application is published, restrict the number of connections to a maximum of 200. At a command prompt, type:

ctxcfg -l max=200

To display the load factor

If you tuned the load using ctxcfg -k loadfactor, you can display the current load factor setting for a server using the ctxcfg -g command.

1. At a command prompt, type: ctxcfg -g | grep loadfactor

To display the load

You can display the load for a particular server or application using the ctxqserver -app command.

1. At a command prompt, type: ctxqserver -app [application-name | server-name]
where *application-name* is the name of a published application, and *server-name* is the name of the server for which you want to display the load.
Troubleshooting Load Balancing

If users frequently disconnect and reconnect to sessions on load balanced servers rather than logging off, the load may not be distributed evenly among the servers.

Also, if users are using plugins that support session sharing and they start multiple applications, the plugins will attempt to start subsequent applications within the existing session, rather than create a new session. This may lead to uneven application load distribution among the servers.
Configuring ICA Gateways

For servers or client devices to contact XenApp servers on a different network, an ICA gateway must be configured.

The master browser maintains the browse list and periodically receives updates from other browsers (XenApp servers) on the same network. The exchange of information between the master browser and the other browsers takes place over the local subnet. To communicate and exchange information with other networks, you must establish an ICA gateway on the participating networks.

If you have more than one network subnet—for example, if you use a router or a WAN to connect two networks—you need to set up an ICA gateway to allow the master browsers on each network to share information about available servers and published applications.

An ICA gateway consists of at least two XenApp servers. The local server is responsible for contacting the other network and setting up a link between the master browsers on each network. The remote server is a server on the other network that communicates with the local server to establish the ICA gateway.

To display the ICA gateways configured on a server
1. Log on to the server as an administrator.
2. At a command prompt, type:

   ctxbrcfg -g list

To add or remove an ICA gateway
1. Log on to the server as an administrator.
2. At a command prompt:

<table>
<thead>
<tr>
<th>To</th>
<th>Use the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a gateway host name or IP address to the list.</td>
<td>ctxbrcfg -g add=gateway</td>
</tr>
<tr>
<td>Remove a gateway host name or IP address from the list.</td>
<td>ctxbrcfg -g remove=gateway</td>
</tr>
</tbody>
</table>

Note: You can also use the ctxqserver -gateway command to display information about the ICA gateways known to each server on the network; see the Command Reference for details.
Using ICA with Network Firewalls

Network firewalls can allow or block packets based on the destination address and port. If you are using ICA through a network firewall, use the information provided in this topic to configure the firewall.

**ICA TCP/IP Connection Sequence**

1. The client device sends a packet to port 1494 on the XenApp server requesting a response to a randomly selected port above 1023.

2. The server responds by sending packets to the client device with the destination port set to the port requested in Step 1.

If you have a firewall or other TCP/IP network security, configure it to allow TCP/IP packets on port 1494 to pass to servers on your network.

Configure the firewall to allow TCP/IP packets on outbound ports above 1023 to pass to client devices.

If the firewall is not configured to pass ICA packets, users may receive the error message “There is no route to the specified subnet address.”

**Note:** You can configure the XenApp server to use a different port number from 1494, using the ctxalt -a command. Plugins must be configured to use the different port; see the documentation for the plugins you plan to deploy.

**The ICA Browser**

The ICA Browser Service uses UDP port 1604. Browser responses are sent to a high port number above 1023.

The firewall must be configured to allow inbound UDP port 1604 packets to XenApp servers for load balancing and ICA server browsing to function correctly.

Citrix recommends you use the XML Service to avoid passing UDP through the firewall; for more information see Using the Citrix XML Service.

**Caution:** Allowing untrusted access to the ICA Browser Service entails some security risk. Configure the firewall to pass browser data only if load balancing and server browsing across the firewall are essential.
ICA Browsing with Network Address Translation

Some firewalls use IP address translation to convert private (intranet) IP addresses into public (Internet) IP addresses. Public IP addresses are called "external" addresses because they are external to the firewall, whereas private IP addresses are said to be "internal" addresses.

Hosts on the internal network have one set of addresses that is translated to another set when passing through the firewall. For example, an internal host has a private address 192.168.12.3. The firewall translates this into a different public address such as 206.103.132.20.

To browse published applications and XenApp servers, the plugin contacts a server and requests the address of the master browser. If the plugin is external to the firewall, it must be configured to use the public address of a XenApp server. The server returns the IP address of the current master browser to the plugin. By default, the IP address returned to the plugin is the internal address.

If the client device is outside the firewall and the firewall is configured for address translation, the IP address returned to the plugin for the master browser will be incorrect.

Returning External Addresses to Client Devices

Use the ctxalt command to configure the browser to return the external IP address to client devices. You must configure every server that can be elected as the master browser.

The ctxalt command sets an alternate address for the browser on that computer. The external address for the server is specified as the alternate address. The plugin requests the alternate address when contacting servers inside the firewall. The alternate address must be specified for each server.

To set an alternate address for a server

1. Determine the correct external IP address.

2. At a command prompt, type ctxalt -a browser-address alternate-address.

3. Repeat on each server.

In addition to specifying the alternate address on the server, the plugin must be configured to request the alternate address when contacting the master browser. For information about configuring plugins to request the alternate address, see the documentation for the plugins you plan to deploy.
Configuring the TCP/IP Port Number

By default, the TCP/IP port number used by the ICA protocol is 1494. You can change the port number using the ctxcfg command with the -P option.

The port number should be in the range 1024-65535 and must not conflict with other port numbers being used. Whenever the port number is changed, the server must be restarted for the new value to take effect.

Important: If you change the port number on the server, you must also change it on every plugin that will connect to that server. For instructions about changing the port number on client devices, see the documentation for the plugins that you plan to deploy.

To display the current TCP/IP port number

1. Log on to the server as an administrator.
2. At a command prompt, type:

   
   $ ctxcfg -P list

   

To change the TCP/IP port number

1. Log on to the server as an administrator.
2. At a command prompt:

   
   To set
   The port number to the value \textit{num}
   The port number back to the default, 1494
   Use the command
   ctxcfg -P set=num
   ctxcfg -P reset

   

Examples

To set the TCP/IP port number to 5000:

cctxcfg -P set=5000

To reset the port number to 1494:

cctxcfg -P reset
Configuring Session Status Logging

This topic explains how to configure the logging of session events in the system log file. Using the ctxcfg command with the -k option, you can control the logging of session logons, logoffs, disconnects, and reconnects. To do this, use the following keywords: logonlogging, logofflogging, reconnectlogging, and disconnectlogging. Set each keyword to one of the following values:

0. Do not log the event.

1. Enable the short form of logging. This provides default syslog information, such as the date and time, and the user name.

2. Enable detailed logging. This provides default syslog information, the user name, the session id, client device name, and information about what is running, such as a published application name or desktop.

To configure session event logging

1. Log on to the server as an administrator.

2. At a command prompt:

<table>
<thead>
<tr>
<th>To</th>
<th>Use the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log session logons</td>
<td>ctxcfg -k logonlogging={0</td>
</tr>
<tr>
<td>Log session logoffs</td>
<td>ctxcfg -k logofflogging={0</td>
</tr>
<tr>
<td>Log session reconnects</td>
<td>ctxcfg -k reconnectlogging={0</td>
</tr>
<tr>
<td>Log session disconnects</td>
<td>ctxcfg -k disconnectlogging={0</td>
</tr>
</tbody>
</table>

Example

To enable detailed logging for reconnects, type:

ctxcfg -k reconnectlogging=2
Configuring the Operating System for a Large Number of Connections

You may need to configure your system for a large number of connections. A large number of connections consumes resources; therefore, it is important that you choose the optimum values for your environment. Configuration instructions differ, depending on your operating system. For each operating system, a large number of connections is defined, as follows:

<table>
<thead>
<tr>
<th>Operating Systems</th>
<th>No. of connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris</td>
<td>30+</td>
</tr>
<tr>
<td>HP-UX</td>
<td>10+</td>
</tr>
<tr>
<td>AIX</td>
<td>30+</td>
</tr>
</tbody>
</table>
Configuring a Solaris System

If you are configuring a Solaris system to support more than 30 connections, you may need to configure the total number of pseudo-terminals or increase the limits on the number of files. You may also need to increase the number of concurrent CDE sessions that can be run. By default, this number is limited.

For further information about how best to configure your system, see your Solaris documentation.

Caution: Be careful when using the set command in /etc/system—it causes unchecked, arbitrary, and automatic changes to variables in the kernel. If the server will not start and you suspect a problem with /etc/system, use the boot -a command. See the boot man page for more information.
Changing the Number of Pseudo-Terminals

In a large number of ICA connections, the number of ptys (pseudo-terminals) can easily surpass the default value (usually a session has at least one pty).

To change the number of pseudo-terminals

1. Add the following lines to the /etc/system file:

   # set limit on pseudo-terminals
   set pt_cnt = 500

   **Note:** Do not set pt_cnt above 3000.

2. Shut down the server—for example, type:

   init 0

3. Restart the server:

   boot -r
Increasing File Limits

There is a limit to the number of files a process can have open; the default value is 64. To increase the file limits for an individual process, use the ulimit command in a script before launching the process, as in the following example.

To change the file descriptor limits for all processes

1. Add the following lines to the /etc/system file:

   ```
   # set hard limit on file descriptors
   set rlim_fd_max = 4096
   # set soft limit on file descriptors
   set rlim_fd_cur = 256
   ```

2. Restart the server:

   ```
   boot -r
   ```
Increasing the Number of Concurrent CDE Sessions

With the default configuration of Solaris, there is a limit to the number of concurrent CDE sessions that can be run (approximately 60, depending upon session configuration). This is due to the tooltalk database reaching a limit of available file descriptors. However, you can increase the number of possible concurrent CDE sessions.

The procedure for increasing the limit on concurrent CDE sessions depends on whether or not the file /usr/dt/bin/rpc.ttdbserverd is a link to /usr/openwin/bin/rpc.ttdbserverd. Check this before you make any changes.

To increase the limit on concurrent CDE sessions if the file is link

1. Remove the file /usr/dt/bin/rpc.ttdbserverd:
   
   ```
   rm /usr/dt/bin/rpc.ttdbserverd
   ```

2. Replace the link with the following script file. In this example, ulimit is used to increase the limit to 1024:
   
   ```
   #!/bin/sh
   ulimit -n 1024
   exec /usr/openwin/bin/rpc.ttdbserverd
   ```

3. Make the file executable:
   
   ```
   /bin/chmod a+x /usr/dt/bin/rpc.ttdbserverd
   ```

4. Kill the currently running rpc.ttdbserverd process.

5. Restart rpc.ttdbserverd to ensure the new limit is applied.

To increase the limit on concurrent CDE sessions if the file is not a link

1. Edit the file /usr/dt/bin/rpc.ttdbserverd and change the limit.

2. Kill the currently running rpc.ttdbserverd process.

3. Restart rpc.ttdbserverd to ensure the new limit is applied.
If the Database Gets Corrupted

Files in /TT_DB occasionally get corrupted, and messages such as the following may appear in your /var/adm/messages file:

/usr/dt/bin/ttsession[11627]: Error: rpc.ttdbserverd on 127.0.0.1 is not running

/usr/dt/bin/ttsession[11627]: _Tt_db_client::connectToDb(): fcntl(F_SETFD): Bad file number

/usr/dt/bin/ttsession[11627]: _Tt_db_file::_Tt_db_file(): _file_cache->insert(<your hostname>/etc/tt/types.xdr), dbStatus 16

If you suspect that the database is corrupted, do the following:

1. Remove all the files in the /TT_DB directory
2. Kill the currently running rpc.ttdbserverd process.
3. Restart rpc.ttdbserverd to ensure the new limit is applied.

Restarting the server automatically creates new database files.
Configuring an HP-UX System

This topic provides guidelines for configuring your HP-UX system for more than 10 connections.

For further information about how best to configure your system, see the relevant white papers on Hewlett-Packard’s Web site at http://docs.hp.com/.
To configure your HP-UX system for more than 10 connections

1. Choose System_Admin from the Application Manager.
2. Choose Sam.
3. Enter the root password at the prompt. The System Administration Manager dialog box appears.
4. Choose Kernel Configuration.
5. Choose Configurable Parameters. The Kernel Configuration dialog box appears.
6. Update your system with the following settings. This tunes your system to run multiple processes (each of which may have many threads and open files) and increases the number of users that can log on concurrently.

   **Note:** Change the value of maxusers first—this allows you to update the other settings.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maxusers</td>
<td>1000 (or as</td>
<td>Allocates system resources for macros on expected maximum users.</td>
</tr>
<tr>
<td></td>
<td>required)</td>
<td></td>
</tr>
<tr>
<td>dbc_max_pct</td>
<td>20</td>
<td>Maximum dynamic buffer cache.</td>
</tr>
<tr>
<td>max_thread_proc</td>
<td>2048</td>
<td>Maximum threads per process.</td>
</tr>
<tr>
<td>maxfiles</td>
<td>2048</td>
<td>Soft limit of files per process.</td>
</tr>
<tr>
<td>maxfiles_lim</td>
<td>2048</td>
<td>Hard limit of files per process.</td>
</tr>
<tr>
<td>maxssiz</td>
<td>401604608</td>
<td>Maximum process storage segment size.</td>
</tr>
<tr>
<td>maxssiz_64bit</td>
<td>1073741824</td>
<td>Maximum process storage segment size—64-bit.</td>
</tr>
<tr>
<td>maxswapchunks</td>
<td>4096</td>
<td>Maximum swap space configurable on the system.</td>
</tr>
<tr>
<td>nflocks</td>
<td>3461</td>
<td>Maximum number of file locks on the system.</td>
</tr>
<tr>
<td>npty</td>
<td>2000</td>
<td>Maximum number of ptys (pseudo-terminals) on the system.</td>
</tr>
</tbody>
</table>
If you are configuring an AIX system to support more than 30 connections, you may need to configure the total number of pseudo-terminals or increase the limits on the number of processes per user.

For further information about how best to configure your system, see the relevant white papers on IBM’s Web site at: http://www.ibm.com/.
Changing the Number of Pseudo-Terminals

In a large number of ICA connections, the number of ptys (pseudo-terminals) can easily surpass the default value (usually an ICA session has at least one pty).

To change the number of pseudo-terminals

1. Log on as root on the server that you want to configure.
2. Type smit. The System Management Interface Tool dialog box appears.
3. Choose Devices.
4. Choose PTY.
5. Choose Change/Show Characteristics of the PTY.
6. Change the number of Pseudo-Terminals.
7. Select OK. pty0 changed appears.
Increasing the Number of Processes Per User

On AIX, by default, there is a limit to the number of processes a user can have running simultaneously. The default is 128 processes per user.

If a user runs out of processes, the user cannot run any commands or log off from the session until more processes are made available. For example, this situation may occur in a training scenario where several users are logged on to the server using only the one training user id.

You can increase the number of processes a user can run simultaneously using SMIT.

To increase the number of processes per user

1. Log on as root on the server.
2. Type smit. The System Management Interface Tool dialog box appears.
3. Choose System Environments.
5. Increase the value of Maximum number of PROCESSES allowed per user (Num).
Configuring Non-English Language Support

XenApp dialog boxes and system messages appear in US English, which is the default language. However, you can run XenApp in a non-English locale by configuring the server so that dialog boxes and system messages appear in French, German, or Spanish. The XenApp Login screen, user dialog boxes, and system messages that appear in ICA sessions appear in the language appropriate to your users.

Configuring XenApp for non-English language support is a simple process that involves editing the ctxenv.sh script to change the locale in which the server runs. For information about configuring the server for non-English language support, see Changing the Locale.

Before you edit ctxenv.sh, the server starts in the currently active locale; that is, the server starts in the locale that is active when you log on to the console. If this locale provides non-English language support (see below for details of locales that provide non-English language support), ICA connections appear in the appropriate language: French, German, or Spanish. If the currently active locale does not provide non-English language support, ICA connections appear in US English.

To ensure the server uses the appropriate locale, you must edit the ctxenv.sh file and restart the server. If you do not edit ctxenv.sh, the server uses the locale that is active when it starts, and this may produce unexpected results. For information about editing ctxenv.sh, see Changing the Locale.
Which Locales Provide Non-English Language Support?

XenApp provides non-English language support for the following locales:

- **French** ISO 8859-1, ISO 8859-15
- **German** ISO 8859-1, ISO 8859-15
- **Spanish** ISO 8859-1, ISO 8859-15

For example, if the server is configured to use the French ISO 8859-1 locale, French dialog boxes and system messages appear to client users.
Limitations of Non-English Language Support

Only French, German, or Spanish language support is provided. Although XenApp will run in other locales, no language support is provided. For example, the server can run in an Italian locale and support Italian keyboards, but dialog boxes and system messages appear in US English, not Italian.

If you configure the server for non-English language support, this localizes only the Login screen, dialog boxes, and system messages that appear within ICA sessions. This does not localize the commands you use to administer XenApp, or the man pages and shell scripts.

In addition, only the messages within dialog boxes appear in the appropriate language. Other information, such as dates and times, may be incorrect. For example, an incorrect date and time may appear in the Reconnect dialog box.

Getting More Information about Language Support

To fully localize your installation in a language other than US English, you need to:

- Deploy appropriate language versions of the plugin software. You can download plugins from http://www.citrix.com/download/. For information about how to install, configure, and deploy plugins to end-users, see the appropriate plugin documentation.

- Deploy appropriate language versions of applications—for information about how to publish applications, see Publishing Applications and Desktops.

- If your users are using non-English keyboards, ensure they select the appropriate keyboard in the plugin software. For information about supported keyboards, see Configuring Non-English Language Support; for information about selecting keyboards, see the documentation for the appropriate plugin.
Changing the Locale

To configure the server for non-English language support, you edit the ctxenv.sh script to change the locale in which the server runs. This script is located in the following directories:

On HP-UX and Solaris:

/opt/CTXSmf/slib directory

On AIX:

/usr/lpp/CTXSmf/slib directory

To make this process as simple as possible, the ctxenv.sh script includes standard entries for commonly used locales. To change the locale in which the server runs, you uncomment the line for the appropriate locale in ctxenv.sh.

The following example shows the standard entries in ctxenv.sh on the Solaris platform:

```
# Reset all environment variables so inherited values are ignored.
# Uncomment the next line and the line for your chosen locale.
# LANG=LC_MESSAGES=LC_TIME=LC_NUMERIC=LC_MONETARY=LC_COLLATE=LC_ALL=

# English (ASCII codset)
# LANG=C

# French - Solaris 2.6/7 (ISO 8859-1 codset)
# LANG=fr

# German - Solaris 2.6/7 (ISO 8859-1 codset)
# LANG=de

# Spanish - Solaris 2.6/7 (ISO 8859-1 codset)
# LANG=es

# French - Solaris 9 (ISO 8859-1 codset)
# LANG=fr_FR.ISO8859-1:LC_MESSAGES=fr

# German - Solaris 9 (ISO 8859-1 codset)
# LANG=de_DE.ISO8859-1:LC_MESSAGES=de

# Spanish - Solaris 9 (ISO 8859-1 codset)
# LANG=es_ES.ISO8859-1:LC_MESSAGES=es

#export all environment variables
export LC_ALL LC_MESSAGES LC_TIME LC_NUMERIC LC_CTYPE LC_MONETARY LC_COLLATE LANG
# bld-iso12.bld-iso12-BuildClient.50120 # 4570
`
To change the locale

1. Log on to the server as an administrator.

2. Stop the server using the ctxshutdown command.

3. Open the ctxenv.sh file and locate the following lines:

   # Reset all environment variables so inherited values are ignored.

   # UNCOMMENT THE NEXT LINE and the line for your chosen locale.

   #LANG=;LC_MESSAGES=;LC_TIME=;LC_NUMERIC=;LC_CTYPE=;LC_MONETARY=;LC_COLLATE=;LC_ALL=

4. Remove the # character from the start of the line beginning with #LANG=.

5. Find the line containing the locale you want to apply and remove the # character from the start of this line. Note that you can apply only one locale. For example, to choose the French ISO 8859-1 locale, remove the # character from the following line:

   #LANG=fr_FR.ISO8859-1;LC_MESSAGES=fr

6. Save the changes to the ctxenv.sh file.

7. Start the server using the ctxsrv start all command.

   The server starts in the appropriate locale.

Example: To use the German ISO 8859-15 locale

1. Remove the # character from the start of the following line:

   #LANG=;LC_MESSAGES=;LC_TIME=;LC_NUMERIC=;LC_CTYPE=;LC_MONETARY=;LC_COLLATE=;LC_ALL=

2. Include the following line:

   LANG=de_DE.ISO8859-1;LC_MESSAGES=de
If the Locale You Require Is not Listed in ctxenv.sh

If the locale you require is not included in the ctxenv.sh script, you can edit ctxenv.sh to include this locale. Make sure you remove the # character from the start of the #LANG= line (as described in the above procedure), and that you apply only the one locale.

Note: Only the locales listed in Which Locales Provide Non-English Language Support? provide non-English language support. If you include a locale that is not listed, US English appears by default.
Troubleshooting Non-English Language Support

Cannot Find ctxenv.sh

The ctxenv.sh script is located in the following directories:

For HP-UX and Solaris:

/opt/CTXSmf/slib

For AIX:

/usr/lpp/CTXSmf/slib

After Editing ctxenv.sh, Information Still Appears in English

- If you configure the server to display in French, German, or Spanish, only the Login screen, user dialog boxes, and system messages that appear in ICA sessions appear in the appropriate language. The commands that you use to administer XenApp, and the man pages and shell scripts remain in US English. For more information about configuring your server console for non-English language support, see your UNIX software documentation.

- If you select a locale that is not supported by XenApp, US English is used by default.

Dialog Boxes and System Messages Appear in the Wrong Language

- Check that the ctxenv.sh script was edited correctly, otherwise the server uses the locale that is active when the server starts, and this may produce unexpected results.

- Ensure that users’ start-up scripts do not contain locale settings. If a user’s start-up script overrides the server’s locale setting, information may appear in more than one language.

Dates and Times Are Incorrect

Only the messages in user dialog boxes are in French, German, or Spanish. This means that the date and time for the locale may be incorrect and should, therefore, be disregarded. For example, an incorrect date and time may appear in the Reconnect dialog box.
The Locale Selection Menu Does not Appear on the Login Screen

XenApp supports only the use of one locale at a time, and does not offer per-session selection.

How Do I Find Out My Current Locale?

Use the locale command to display information about the current locale environment. For more information about the locale command, see the locale man page or consult your UNIX software documentation.
Using the Citrix XML Service

The Citrix XML Service for XenApp for UNIX runs as a daemon on all servers in a server farm. The key features and benefits of using the XML Service include:

**Web-based application deployment.** Using the XML Service, you can deploy applications published on XenApp servers to your users through the Web. The XML Service communicates information about the UNIX applications published in a server farm to the Citrix Web Interface. The Web Interface provides users with an HTML-based presentation of the server farm. Users can access their published applications using a standard Web browser. You can specify the name and icon used to display the link to each application in the Web page and the default window settings for the application when run. For more information about the Web Interface, see the *Web Interface Administrator’s Guide*.

**Ticketing.** The XML Service provides support for ticketing, which offers enhanced authentication security by eliminating user credentials from the ICA files sent from the Web server to client devices. The use of the Web Interface's ticketing feature eliminates the danger of an attacker intercepting user credential information and using this to access a XenApp server. For more information about how to use ticketing in your Web Interface deployment, see the *Web Interface Administrator’s Guide*.

**HTTP browsing.** You can provide your users with HTTP (HyperText Transport Protocol) browsing. The plugin uses HTTP to communicate with the Citrix XML Service to fulfill browser requests. HTTP browsing uses the standard HTTP port on the firewall—port 80—to allow users to browse applications and servers that exist on the other side of a firewall. This means that, provided port 80 is not being used by a Web server running on the server, there is no need to open an additional port on the firewall for browser requests.

**SSL Relay support.** The XML Service provides SSL Relay support. SSL Relay provides the ability to secure data communications using Version 4.0 of the Secure Sockets Layer (SSL) protocol. SSL provides server authentication, encryption of the data stream, and message integrity checks. You can use SSL Relay to secure communications in a Web Interface deployment between the Web server and the XenApp server. For more information about configuring and using SSL Relay, see the *Citrix XenApp SSL Relay for UNIX Administrator’s Guide*.

**Server Farm Considerations**

For XenApp for UNIX servers to be included in a farm, they need to be on the same subnet or connected by Citrix ICA gateways. For more information, see *Multiple Farms and Subnet Considerations*.

You can make applications published in XenApp for UNIX server farms appear in the same location as applications published on XenApp for Windows farms. To do this, you use the multiple server farm functionality in the Web Interface. Multiple server farm functionality is transparent to users because they are not informed that their application set is an aggregation from multiple server farms. Applications from multiple server farms appear in the same way as a single farm; folders appear first, followed by application icons. For more information, see the *Web Interface Administrator’s Guide*. 
Getting Started with the Citrix XML Service

The Citrix XML Service is included automatically when you install XenApp for UNIX, and the XML process starts automatically. If you create a server farm, the XML Service runs on each server in the farm. Configuration information required by the XML Service is stored in ctxxmld.cfg.

Typically, little or no configuration is required to get the XML Service up and running quickly in your installation. However, you may need to configure the XML Service to use port numbers other than the defaults or to enable DNS address resolution. This section explains what configuration is required and where to find more information.

Configuring display settings. You can configure your applications for use with the Web Interface using the ctxappcfg command. Using ctxappcfg, you can configure display settings that include the name of the folder containing the application and the icon that the Web Interface displays, and the window size and color depth. For more information about configuring application display settings, see Publishing Applications and Desktops.

Configuring the XML Service port. By default, the Web server communicates with the XML Service using port 80. If port 80 is already in use on the server running the XML Service, assign the XML Service to an unused port. See Configuring the Server Port for more information.

Configuring the SSL Relay port. To enable your users to make SSL-secure connections to applications through the Web Interface, you must configure the XML Service for use with SSL Relay. To do this, you use the ctxappcfg command to specify whether SSL is used to secure connections on all published applications or on a particular application only (see Publishing Applications and Desktops for more information). If you are not using TCP port 443, which is the standard port for SSL-secured communications, you must specify the port number that SSL Relay listens for connections on using the ctxnfusesrv command. For information about how to do this, see Configuring the XML Service for Use with SSL Relay.

Note: If you configured a particular server to be the master browser, Citrix recommends that you direct the Web Interface to this server. For more information about the ICA browser, see XenApp for UNIX and the ICA Browser Service. Also, if plugins are using HTTP browsing, it is best to direct plugins to the master browser server. See your plugin documentation for more information.
Starting and Stopping the Citrix XML Service

When you start and stop XenApp, the Citrix XML Service automatically starts and stops. Using the ctxsrv command, you can start and stop the Citrix XML Service on the local server.

To start the Citrix XML Service

1. Log on to the server as an administrator.
2. At a command prompt, type:
   
   ctxsrv start msd

   Starting a server causes an election, and the master browser may change. The master browser takes some time to acquire information about applications available on the farm. If the Citrix XML Service is started at the same time as a XenApp server, it can take up to 10 minutes before these applications are visible through the Web Interface.

To stop the Citrix XML Service

1. Log on to the server as an administrator.
2. At a command prompt, type:
   
   ctxsrv stop msd
Configuring the Server Port

By default, the Web Interface communicates with the Citrix XML Service using port 80. If port 80 is already in use on the server running the XML Service, assign the XML Service to an unused port.

Note: The XML Service port number must be unique. If the port is already in use by another process, results may be unpredictable. You must configure the Web Interface to use the same port number as you specified for the XML Service—see the Web Interface Administrator’s Guide for information about how to do this.

To configure the Citrix XML Service port

1. Log on to the server as an administrator.

2. At a command prompt, type:

   `ctxnfusesrv -port portnumber`

   where *portnumber* is an unused port; for example, 8080.

   Note: You must restart the XML Service for the new port to be used.

To display the current port number

1. At a command prompt, use ctxnfusesrv with the -l (list) option: `ctxnfusesrv -l`
Configuring the XML Service for Use with SSL Relay

SSL Relay is included automatically when you install XenApp for UNIX.

To allow users who connect to the server through the Web Interface to make SSL-secure connections to applications, you must configure the XML Service for use with SSL Relay. To do this you use the:

- ctxappcfg command to specify whether SSL is used to secure connections on all published applications or on a particular application only. ctxnfusesrv command to specify the port number on which SSL Relay listens for connections. You need to run this command only if you are not using TCP port 443, which is the standard port for SSL-secured communications. The SSL Relay port number you specify must be the same on every server in the farm.

For more information about configuring and using SSL Relay, see the *Citrix XenApp SSL Relay for UNIX Administrator's Guide*.

**To configure the SSL Relay port number**

1. Log on to the server as an administrator.

2. If SSL Relay listens for connections on a port other than 443, specify this port number. At a command prompt, type:

   `ctxnfusesrv -ssl-port port-number`

   where *port-number* is the port number on which SSL Relay listens for connections. For example, if SSL Relay listens on port 444, type:

   `ctxnfusesrv -ssl-port 444`

**Troubleshooting SSL**

If you configured your server to use NIS for name resolution, the server cannot support SSL-enabled ICA connections because NIS does not supply the fully qualified domain name (FQDN). The FQDN is required by the XML Service to direct requests from the Web Interface and client devices.

To solve this problem, configure the server to use DNS, in preference to NIS, for name resolution, because DNS supplies the FQDN.
Configuring DNS Address Resolution

By default, servers reply to browsing requests with an IP address. However, a server can respond with the fully qualified domain name. This feature, called Domain Name System (DNS) address resolution, is available to client devices using the XML Service. In most situations, the use of IP addresses works well and with less overhead.

You can enable DNS address resolution using the ctxnfusesrv -dns command.

**To enable DNS address resolution**

1. Log on to the server as an administrator.
2. At a command prompt, type:
   
   `ctxnfusesrv -dns enable`

   **Note:** If DNS addressing is enabled, client devices can connect reliably to servers only if they can resolve the fully qualified domain name. If the plugin is not configured correctly, it cannot connect. Ping a server with its DNS host name to verify this.

**To display the current DNS address resolution setting**

You can display the current DNS address resolution setting using ctxnfusesrv and the -l (list) option.

1. At a command prompt, type: `ctxnfusesrv -l`
Using Client Drive Mapping

The client drive mapping feature enables users to access their local drives from within an ICA session. When a user makes an ICA connection to a XenApp server, the user’s local drives are mounted automatically, such as floppy disk drives, network drives, CD-ROM drives, and hard disk drives.

These drives are available for the duration of the session. When a session is disconnected, all the mapped drives belonging to the session are released immediately. If you shadow a user’s session using ctxshadow, you can also access the local, mapped drives belonging to the shadowed session.

For users to take advantage of client drive mapping:

- Users must be running Version 6.0 or later plugins.

- Use the ctxcfg command to enable client drive mapping. By default, the client drive mapping feature is disabled because it consumes server resources, and so that you can be certain that no one is moving files between the server and client devices.
Enabling Client Drive Mapping

By default, when you install XenApp, client drive mapping is disabled. Therefore, before users can take advantage of this feature, you must enable it on the server. When you enable client drive mapping, you must choose whether to enable the mapped drives with read-write access or with read-only access.

You use the ctxcfg tool with the -D option to enable client drive mapping.

You can also enable client drive mapping on a global basis using the ctxsrv command. For example, if you need to re-enable client drive mapping after you stop it for all users temporarily during a virus scare. For more information, see Re-Enabling Client Drive Mapping.

**Important:** Client drive mapping can also be configured using options available within the plugin. Therefore, for client drive mapping to work, you must ensure that the settings in the plugin are consistent with the settings on the XenApp server. To enable client drive mapping, you must enable it in the plugin, and on the server, and ensure the settings do not conflict. For example, if the plugin is configured to mount only drive C, mounting drive A on the server will have no effect. For more information about configuring client drive mapping in the plugin, see the documentation for the appropriate plugin.

**Note:** To use client drive mapping when running XenApp for UNIX on the AIX operating system, ensure option nfs_use_reserved_ports is set to 1 using the nfso command.

**To enable client drive mapping**

1. Log on to the server as an administrator.

2. At a command prompt, type:
   
   `ctxcfg -D enable,access={ro|rw}`

   where ro is read-only access, and rw is read-write access.

When client drive mapping is enabled, it is enabled for all users and all their available local drives. However, you can restrict access on a user or group level basis using the ctxsecurity security command. For example, to prevent anonymous users (the ctxanon group) from using client drive mapping, use the ctxsecurity command to deny this group access.

You can also restrict user access to specific drives using the ctxmount command. For example, you can configure client drive mapping so that users can access only drive C. You can do this for all users or for particular users.

**Note:** The access policy you implement using ctxcfg takes precedence over any settings configured using ctxmount, including any settings in the ctxsession.sh file. For example, if you enable access as read-only using ctxcfg, this cannot be overridden using ctxmount.
Configuring Access to Specific Drives

When you enable client drive mapping using ctxcfg, all the local drives available to a user are mapped. However, you can configure access to particular mapped drives using the ctxmount command, which you include in the ctxsession.sh script. You can do this for particular users or for every user who connects to the server.

For example, you can configure the system so that in an ICA session:

- The user Fred cannot access drive A
- Fred’s drive C is read-only
- All users cannot access drive C
- All users’ drives A are read-only

If you configure access to specific drives for particular users the procedure you use differs, depending on whether or not you trust those users.

To use the ctxmount command, you modify it within the ctxsession.sh script. The ctxmount command is contained within ctxsession.sh because ctxmount affects only the session in which it runs. ctxsession.sh runs after a user logs on, so you can use it to customize the local environment for a session.

**Note:** Settings configured using ctxcfg take precedence over any settings configured using ctxmount. For example, if you enable read-only access to mapped drives using ctxcfg, read-write access cannot be granted using ctxmount.

You can also configure access to client drive mapping on a user or group level basis, using the security function ctxsecurity.
To configure access to specific drives for every user

Use this procedure to configure access to specific drives for every user who logs on to the server.

1. Log on to the server as an administrator.
2. Open the ctxsession.sh script and locate the following line:

   $CTXMOUNT

3. Update the ctxmount command:

   $CTXMOUNT [-d | -ro] [drivelist]

   The following table explains the options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Use this to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>Disconnect a drive.</td>
</tr>
<tr>
<td>-ro</td>
<td>Configure access to a drive as read-only. If you specify a currently connected drive, this drive is made read-only.</td>
</tr>
<tr>
<td>drivelist</td>
<td>Specify the drive letters to which you want to configure access: (A B C ... Z) or all to specify all available drives. If you do not specify a drivelist, the default of all is used.</td>
</tr>
</tbody>
</table>

Examples

- To connect all drives as read-only, use the command:

  $CTXMOUNT -ro

- To connect drive C only, use the command:

  $CTXMOUNT C

- To connect all drives except drive C, use the commands:

  $CTXMOUNT all
  $CTXMOUNT -d C

- To disconnect all drives, use the command:
To configure access to specific drives for every user

$CTXMOUNT -d

- To disconnect drives M, N, and T, use the command:

$CTXMOUNT -d M N T
To configure access to specific drives for a particular trusted user

If you trust your users, use the following procedure to allow users to configure access to specific drives.

**Important:** With this method users can overwrite these settings using the ctxmount command.

1. Log on to the server as an administrator.

2. Open the ctxsession.sh script and locate the following lines:

```
#if [ -f $HOME/.ctx.session.sh ] ; then
  . $HOME/.ctx.session.sh
#fi
```

3. Under here, insert lines similar to the following (in this example, the user “bill” is given read/write access to drives A, C, and E, “mandy” is given read-only access to drive C, and for all other users drives are disconnected):

```
   case $USER in
     bill)
        ctxmount ACE
     
     mandy)
        ctxmount -ro C
   
   esac
```

```
To configure access to specific drives for a particular trusted user

*)

cctxmount -d

;;;

esac

Note: This script is run for every session.
Users can modify the .ctx.session.sh file and run any commands that they choose.
To configure access to specific drives for a particular untrusted user

If you do not trust your users, use the following procedure to configure access to specific drives. With this method, users cannot overwrite these settings using the ctxmount command.

1. Log on to the server as an administrator.

2. Open the ctxsession.sh script and locate the following lines:

   #if [ -f $HOME/.ctx.session.sh ] ; then
   #. $HOME/.ctx.session.sh
   #fi

3. Remove the # character from the start of each line, so that these lines are no longer commented out.

4. In the user’s home directory, create a file called .ctx.session.sh.

5. In the .ctx.session.sh file, include the ctxmount command with the appropriate options:

   ctxmount [ -d | -ro ] [ drivelist ]

Note:

If you do not trust your users, and do not want them to use client drive mapping, except as you define here, do not give them access to a command prompt from which they can run ctxmount. That is, give your users access only to published applications.
Disabling Client Drive Mapping

How you disable client drive mapping depends upon whether you want to disable it for new connections only, or disable it for all connections including any existing ones.

- To disable client drive mapping for new connections only, use the ctxcfg command. Client drive mapping will still be available for existing connections.

- To disable client drive mapping for all connections, including any existing connections, use the ctxsrv stop command. This command immediately stops the client drive mapping process on the server. For example, use this method to immediately disable client drive mapping for all users during a virus scare.

**To disable client drive mapping for new connections**

1. Log on to the server as an administrator.
2. At a command prompt, type:

   ctxcfg -D disable

**To disable client drive mapping for all connections, including existing ones**

1. Log on to the server as an administrator.
2. At a command prompt, type:

   ctxsrv stop cdm

Re-Enabling Client Drive Mapping

How you re-enable client drive mapping depends upon how you disabled it, as follows:

- If you disabled client drive mapping using ctxcfg, use ctxcfg to re-enable it.

- If you disabled client drive mapping on the server using ctxsrv stop, use ctxsrv start to restart it.
To re-enable client drive mapping (if disabled using ctxcfg)

1. Log on to the server as an administrator.

2. At a command prompt, type:

   \texttt{ctxcfg -D enable,access=\{ ro|rw \}}

   where ro is read-only access, and rw is read-write access.

To restart client drive mapping (if disabled using ctxsrv)

1. Log on to the server as an administrator.

2. At a command prompt, type:

   \texttt{ctxsrv start cdm}

Tip: Use ctxcfg -D list to display whether client drive mapping is currently enabled or
disabled. Note, however, that this shows only the enabled or disabled status configured
using the ctxcfg command—it does not display whether client drive mapping is enabled or
disabled using ctxsrv.
Features and Limitations of Client Drive Mapping

These topics provide further information about how client drive mapping works. They tell you about the /ctxmnt directory and the $CTXCLIENT environment variable. They also provide information that you and your users need to know about file names, permissions, and formats, and about the limitations of client drive mapping in this release.
How Does Client Drive Mapping Work?

When you install XenApp, the /ctxmnt directory is created on the server. When client drive mapping is enabled, this directory holds information about clients’ mapped drives for each session that connects to the server.

When a user makes a connection to the server, the user’s drive mappings are held in this directory as:

/ctxmnt/username/default/driveletters

If a user starts additional sessions that run concurrently with the user’s first session, the additional drive mappings are held as:

/ctxmnt/username/$CITRIX_SESSION_ID/driveletters

Each session uses the $CTXCLIENT environment variable to point to the appropriate drive mappings on the server.

For example, within an ICA session the user Fred accesses a file on his hard disk called: C:\accounts\expenses.txt. This file is mapped as /ctxmnt/fred/default/C/accounts/expenses.txt. If Fred starts another session, the session id is used to map additional files and directories; for example, /ctxmnt/fred/20/C/accounts/payments.txt.
File Names

File names permitted in one operating system may not be permitted in another. For example, the Windows operating system does not allow file names that match devices. Likewise, some operating systems do not permit file names that contain certain characters, such as: \ / : * ? “ < >. File names containing non-English characters can also appear differently between the client and the server.

Client drive mapping does not take the case of file names into consideration; for example, the files “readme.txt” and “README.TXT” are treated as the same file. Client drive letters, however, are always converted to upper case.

If you are using the Citrix Delivery Clients for Windows, do not use an asterisk (*) within quotation marks in file names. For example, if you want to change directory to “New Folder,” either type the full name of the file, or type:

```
cd /ctxmnt/username/default/driveletter/Ne*
```
File Permissions

File permissions are set at the user name level; therefore, only the user who owns the file can access and update files on their local, mapped drives. You cannot change the permissions on files in the /ctxmnt directory using chmod or chown. Execute permissions cannot be set on any files served by client drive mapping.

Files that are executable locally cannot be executed within a mapped client drive. For example, on a local UNIX computer, you have a file called a.out. When you run ls -l on the local computer, the file permissions are listed as rwxr-xr-x. However, if you run ls -l on the mapped drive, the file permissions are listed as rw-------.

**Caution:** UNIX permissions prevent users from being able to display and access each other’s files. However, if you use ctxcfg -a to allow automatic logon, your users can see directory listings of each others’ files (for example, using the ls command in UNIX) and they can access and display the contents of the files because users are logged on under the same user id. To prevent this, do not use ctxcfg -a with client drive mapping.
File Attributes

File attributes that apply on one operating system may be ignored on another. For example, files that are hidden in Windows may appear when displayed in a different operating system, such as UNIX. DOS file attributes (with the exception of read-only) are ignored in UNIX.
File Formats

Although client drive mapping provides users with access to their local drives, file format conversion does not occur automatically. This means that files stored on local client devices may appear differently in an ICA connection that uses client drive mapping. Similarly, files stored on the server may appear differently when saved to the local client device.

For example, files created on a DOS file system may contain both carriage returns and line feeds as line terminators, while files created on a UNIX system may contain line feeds only.
These topics describe problems that you and your users may experience, or typical questions that may be asked about client drive mapping, and provide possible solutions and answers to these.
Client Drive Mapping Does not Work

The following diagram shows the steps you need to perform on the server if client drive mapping does not work:
Check using:

- ctxcfg -D list
- ps -ef | fgrep ctxcdm
- ctxsecurity cdm -l
- Is /ctxmntUsername/default

Tip: Remember to check also that client drive mapping is enabled on the client, and that these settings are consistent with the settings on the server.
“Invalid Directory” or “Stale File” Error Messages

When a session is disconnected, all the mapped drives belonging to the session are immediately released. However, some applications store the paths of files on which a user recently worked. If a session is disconnected and later reconnected, the path to a file may be invalid in the reconnected session.

For example, in an application running in an ICA connection, Fred edits a file that is mapped as /ctxmnt/fred/default/C/accounts/expenses.txt. However, Fred’s connection breaks and he reconnects the session. This time the system maps the file as /ctxmnt/fred/10/C/accounts/expenses.txt. Therefore, when Fred attempts to access expenses.txt in the application, the path is no longer valid and error messages such as “invalid directory” or “stale file” appear.
Problems Accessing and Updating Files

File names permitted in one operating system may not be permitted in another. For example, the Windows operating system does not allow file names that match devices, so users of Windows clients may experience problems attempting to write files called com1.txt, lpt1, aux, and so on.

Some operating systems do not permit file names that contain certain characters; for example, in Windows these characters are: \ / : * ? “ < >

File names containing non-English characters may also appear differently due to mismatches in the character encoding used by the client and the server. For example, a user has a file on a hard drive called “¼results.txt;” however, when viewing this file in an ICA session the user sees “?results.txt.” To access files that contain characters that are not available on the keyboard, use wildcards; for example, vi *results.txt.
A File Looks Different when Displayed in an ICA Session

File format conversion does not occur automatically. This means that files stored on local client devices may appear differently in an ICA connection that uses client drive mapping. Similarly, files stored on the server may appear differently when saved to the local client device.

For example, a user has a text file on a local Windows client device. When the user displays this file in an ICA connection, “^M appears at the end of each line. This is due to the different text file formats in the operating systems. Therefore, before the user can work with the file, the file format must be converted; for example, using a utility such as “dos2unix.”
NFS Error Messages

You may receive errors relating to NFS when using XenApp for UNIX.

Not Responding Error Message

In the unlikely event that the client drive mapping process on the server is slow in responding, an error message (such as “NFS server CDM server not responding still trying” or “NFS server 127.0.0.1 not responding still trying”) appears.

Normally, this request is fulfilled and the message “NFS server CDM server ok” or “NFS server 127.0.0.1 ok” appears. However, if the problem persists, you must restart the client drive mapping process on the server.

Tip: To interrupt the request and get a command prompt, press CTRL+C or send a SIGINT to the process.

To restart client drive mapping

1. Ensure that there are no users in the /ctxmnt directory (users should not be reading or writing to this directory, nor should it be their current directory). For example, you may want to ask your users to log off from the server; to do this, use the ctxmsg -a command to send a message to all users.

2. Stop client drive mapping. At a command prompt, type:

   ctxsrv stop cdm

3. Restart client drive mapping. At a command prompt, type:

   ctxsrv start cdm

Stale NFS Handle Error Message

If you disconnect while your current directory is within a mapped directory tree and then reconnect, all subsequent accesses to the mapped directories will result in the error message “Stale NFS Handle.” This happens because information about the mapped drive is lost when the drive is disconnected.

In the reconnected session, change directory so that you are no longer in the mapped drive; for example, by typing cd to go back to the home directory.
Command Reference

These topics describe the XenApp for UNIX and XML Service for UNIX command-line utilities.
XenApp Commands

The XenApp commands are as follows:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctx3bmouse</td>
<td>configure 3-button mouse emulation</td>
</tr>
<tr>
<td>ctxalt</td>
<td>alternate address configuration for ICA browsers</td>
</tr>
<tr>
<td>ctxanoncfg</td>
<td>configure anonymous users</td>
</tr>
<tr>
<td>ctxappcfg</td>
<td>configure published applications</td>
</tr>
<tr>
<td>ctxbrcfg</td>
<td>configure ICA browser settings</td>
</tr>
<tr>
<td>ctxcapture</td>
<td>graphics copy and paste (between ICA and local applications)</td>
</tr>
<tr>
<td>ctxcfg</td>
<td>configure server settings</td>
</tr>
<tr>
<td>ctxconnect</td>
<td>connect to a session</td>
</tr>
<tr>
<td>ctxcreatefarm</td>
<td>create a server farm. See ctxfarm.</td>
</tr>
<tr>
<td>ctxdisconnect</td>
<td>disconnect from a session</td>
</tr>
<tr>
<td>ctxfarm</td>
<td>create a farm, join a farm, remove a server from a farm, or change the farm’s secret key and passphrase.</td>
</tr>
<tr>
<td>ctxgrab</td>
<td>graphics copy and paste (from ICA to local applications)</td>
</tr>
<tr>
<td>ctxjoinfarm</td>
<td>join a server farm. See ctxfarm.</td>
</tr>
<tr>
<td>ctxlogoff</td>
<td>log off from a server</td>
</tr>
<tr>
<td>cxtlpr</td>
<td>print to a client printer</td>
</tr>
<tr>
<td>ctxlscfg</td>
<td>configure communication with a license server</td>
</tr>
<tr>
<td>ctxmaster</td>
<td>show master ICA browser</td>
</tr>
<tr>
<td>ctxmount</td>
<td>configures user access to mapped drives</td>
</tr>
<tr>
<td>ctxmsg</td>
<td>send a message</td>
</tr>
<tr>
<td>ctxprinters</td>
<td>list printers installed on the client device</td>
</tr>
<tr>
<td>ctxqserver</td>
<td>display information about servers</td>
</tr>
<tr>
<td>ctxqsession</td>
<td>display session details</td>
</tr>
<tr>
<td>ctxquery</td>
<td>display session details or details in a different format</td>
</tr>
<tr>
<td>ctxquser</td>
<td>display session user details</td>
</tr>
<tr>
<td>ctxreset</td>
<td>reset a session</td>
</tr>
<tr>
<td>ctxsecurity</td>
<td>configure security</td>
</tr>
<tr>
<td>ctxshadow</td>
<td>start a shadowing session</td>
</tr>
</tbody>
</table>
### XenApp Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxshutdown</td>
<td>shut down the server processes</td>
</tr>
<tr>
<td>ctxsrv</td>
<td>start up or stop the server processes</td>
</tr>
</tbody>
</table>
ctx3bmouse

Description

ctx3bmouse configures 3-button mouse emulation.

You may need to use XenApp to deploy UNIX applications that are designed for use with a 3-button mouse. However, many plugins run on devices that have only a 2-button mouse, 1-button mouse, or pointing device available.

To do this, you publish another version of the application for use by these plugins. This version of the application is published using a script file that includes ctx3bmouse settings. The ctx3bmouse command lets users represent a missing mouse button by combining an existing mouse button with a modifier key. For example, a missing button might be simulated by clicking the left mouse button and pressing the SHIFT key.

By running a script file that includes ctx3bmouse settings, you ensure the application is run in a session with the appropriate mouse mappings.

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctx3bmouse missing_button=mouse_button,number_of_modifier_key</td>
</tr>
<tr>
<td>ctx3bmouse -r</td>
</tr>
<tr>
<td>ctx3bmouse -c</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>-r Display mouse mappings for the current session.</td>
</tr>
<tr>
<td>-c Clear all mouse mappings for the current session.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>missing_button</td>
</tr>
<tr>
<td>mouse_button</td>
</tr>
<tr>
<td>number_of_modifier_key</td>
</tr>
</tbody>
</table>

Remarks

With xmodmap it is possible to remap almost any aspect of the keyboard and mouse. Take care when using xmodmap with ctx3bmouse because the combination may be confusing.

Middle mouse button emulation is included in Version 6.20, or later, of the Citrix XenApp Plugin for Hosted Apps for Windows. If users are connecting to a XenApp server using this plugin, disable any ctx3bmouse settings configured on the server.
ctxalt

Description

ctxalt specifies alternate address configuration for ICA browsers

<table>
<thead>
<tr>
<th>Syntax</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxalt</td>
<td>-l</td>
</tr>
<tr>
<td>ctxalt</td>
<td>-d alt_addr</td>
</tr>
<tr>
<td>ctxalt</td>
<td>-a browser_addr alt_addr</td>
</tr>
<tr>
<td>ctxalt</td>
<td>-r addr</td>
</tr>
<tr>
<td>ctxalt</td>
<td>-h</td>
</tr>
</tbody>
</table>

Options

- **-l** List current alternate address configuration.
- **-d** Set the default alternate address.
- **-a** Set an alternate address.
- **-r** Remove an alternate address.
- **-h** Display usage message

Parameters

<table>
<thead>
<tr>
<th>alt_addr</th>
<th>Specifies the alternate address. With the exception of the -r option, all addresses must be supplied in standard IP address format. The -r option also accepts the (case-insensitive) keyword DefaultAddress to erase the default address setting.</th>
</tr>
</thead>
<tbody>
<tr>
<td>browser_addr</td>
<td>Specifies the default alternate address.</td>
</tr>
</tbody>
</table>

Remarks

You must be an administrator to run this command.
## ctxanoncfg

### Description

ctxanoncfg configures anonymous users.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxanoncfg -l [-q]</td>
<td>List current anonymous user settings.</td>
</tr>
<tr>
<td>ctxanoncfg -n number [-b anonymous_user_name] [-t minutes] [-s shell] [-u user-id] [-g group] [-d path] [-q]</td>
<td>Specify the number of anonymous user accounts.</td>
</tr>
<tr>
<td>ctxanoncfg -t minutes [-q]</td>
<td>Change how anonymous user accounts are named. Use this option only when creating new anonymous user accounts—do not use it to change existing accounts.</td>
</tr>
<tr>
<td>ctxanoncfg -clear</td>
<td>Specify the idle time-out period, in minutes, for anonymous user sessions. If there is no activity within this time, a warning message appears stating that the user will be logged off if the session remains inactive for a further five minutes.</td>
</tr>
<tr>
<td>ctxanoncfg -h</td>
<td>Specify a particular shell for anonymous user accounts.</td>
</tr>
<tr>
<td>Parameters</td>
<td></td>
</tr>
<tr>
<td>number</td>
<td>New number of anonymous user accounts.</td>
</tr>
<tr>
<td>anonymous_user_name</td>
<td>New name of anonymous user accounts. By default, account names are in the format anonx where x is a number from 1,2 ... and so on.</td>
</tr>
</tbody>
</table>
Remarks

You must be root to run this command.

You must stop the XenApp process on the server before you configure anonymous users.

See also

ctxshutdown—to stop the XenApp process.
ctxappcfg

Description

ctxappcfg is an interactive command that allows you to publish and configure applications.

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxappcfg</td>
</tr>
</tbody>
</table>

Usage

When you run ctxappcfg, the App Config> command prompt appears and you can enter the following commands:

list

Displays a list of published application names.

publish

Allows you to publish an application. You are prompted for the following details:

Name - the name used to refer to the published application.

Command Line - the command line used to launch the application. To publish the desktop, press ENTER without specifying a command line.

Working Directory - the working directory used by the application. To specify the user's home directory, leave this blank.

Anonymous - whether the application is for use by anonymous or explicit users. Enter yes if the application is for use by anonymous users only, or no if it is for explicit users only.

Description - an optional description that can be displayed on the user's Web page. If the description includes spaces, enclose it within quotes.

Folder - a folder containing the application.

Icon File - the icon file displayed against a published application.

Window Size - the window size and type of window. Specify window size as \texttt{widthxheight}; for example, \texttt{1024x768}; or \% (percentage) of a desktop; for example, \texttt{70\%}. Specify type of window as seamless (the window size is controlled by the client device) or fullscreen (full screen display).

Color Depth - the number of colors used to display the application. Choose from 16, 256, 4bit, 8bit, 16bit, and 24bit.
Enable SSL security - type yes to use SSL to secure connections to this application, or no if you do not want to use SSL.

User name - the user names of users permitted to access this application. Type one user name per line. Enter a blank line to complete the list. If you do not enter any user or group names, the application cannot be published successfully.

Group name - the names of user groups or netgroups permitted to access this application. Type one group name per line. Leave a blank line to complete the list. To denote a netgroup, use an at symbol (@) as the first character of the name; for example @netgroup1. If you do not enter any user or group names, the application cannot be published successfully.

Server name - the names of servers in the farm that will publish this application. Type one server name per line. Leave a blank line to complete the list. To specify all current servers in the farm, type an asterisk (*). To specify all current and future servers in the farm, type a plus sign (+).

`select [name]`

Allows you to configure a published application. If you do not specify the name of the application you want to configure, you are prompted for it. Note that the application name is case-sensitive. After you select an application, the prompt changes to the name of the application and you can enter the following commands:

`list` - lists the configuration details of the selected application.

`set` - allows you to change the configuration. The full syntax is: `set [cmd={cmd_line}, dir={dir_name}, anonymous={yes|no}, enabled={yes|no}, description={description}, folder={folder_name}, window_size={window size}, color_depth={color depth}, ssl_enabled={yes|no}]` —OR— `set server={server_name}, [cmd={cmd_line}, dir={dir_name}]` where the parameters are as follows:

- `cmd` - the command line required for the program to run.
- `dir` - the initial working directory.
- `anonymous` - indicates if the application is for use by anonymous or explicit users.
- `enabled` - indicates if the application is enabled or disabled.
- `description` - the description displayed on the user’s Web page. If the description includes spaces, enclose it within quotes.
- `folder` - the name of a folder containing the program.
- `window_size` - the window size (width x height or percentage of a desktop) and type of window (desktop or seamless).
- `color_depth` - the number of colors used to display the application. Specify 16, 256, 4bit, 8bit, 16bit, or 24bit.
- `ssl_enabled` - specifies whether or not SSL is used to secure connections to the application. Type yes to use SSL, or no if you do not want to use SSL.
server - the name of the server you want to configure. This option applies only to the command line and working directory.

list users - lists the users who are allowed to access the published application.

list groups - lists groups of users who are allowed to access the published application.

add users - adds users who are allowed to access the published application. Type one user name per line. Leave a blank line to complete the list.

add groups - adds groups of users or netgroups who are allowed to access the published application. Type one group per line. Leave a blank line to complete the list. To denote a netgroup, use an at symbol (@) as the first character of the name; for example @netgroup1. Note that if you specify a netgroup, only the presence of a user in a netgroup is checked; the host and domain fields are ignored.

remove users - prevents users from accessing the published application. Type one user name per line. Leave a blank line to complete the list.

select [name]

remove groups - prevents groups of users from accessing the published application. Type one group per line. Leave a blank line to complete the list.

list servers - lists all servers in the farm that publish the application.

add servers - publish the application on another server in the farm. Type one server name per line. Leave a blank line to complete the list. To specify all current servers in the farm, type an asterisk (*). To specify all current and future servers in the farm, type a plus sign (+). Note that an application must be installed on a server before it can be published.

remove servers - remove the published application from one or more servers in the farm. Type one server name per line. Leave a blank line to complete the list.

export icon - export the current icon to a file that you can later view. You are prompted for the file name.

import icon - specify a different icon file for the published application. You are prompted for the file name.

copy - creates a new published application by copying the configuration of the current application. You are prompted to enter a name for the new application. The new configuration is saved and selected automatically.

save - saves the changes you make.

delete - deletes the currently selected application and returns you to the App Config> prompt.

drop - clears the current application and returns you to the App Config> prompt.

help / ? - displays a brief usage message.

exit - exits the command.
ctxappcfg

default

Allows you to display and configure the default settings for all published applications in
the server farm. To change the default settings, use the set command, which has the
following syntax:

set [folder=[folder name], window_size={window size}, color_depth={color depth},
ssl_enabled]

where the parameters are as follows:

folder - the name of a folder containing the published application.

window_size - the window size (width x height or percentage of a desktop) and type of
window (desktop or seamless).

color_depth - the number of colors used to display the application. Specify 16, 256, 4bit,
8bit, 16bit, or 24bit.

ssl_enabled - specifies whether or not SSL is used to secure connections to the
application. Type yes to use SSL, or no if you do not want to use SSL.

export icon - export the current icon to a file that you can later view.

import icon - specify a different default icon file for the published application.

save - saves the changes you make.

drop - clears the current application and returns you to the App Config> prompt.

help / ?

Displays a brief usage message.

exit

Exits the command.

Remarks

You must be an administrator to run this command.

See also

cctxqserver—to list all published applications on the network.
ctxbrcfg

**Description**

ctxbrcfg configures ICA browser settings.

**Syntax**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxbrcfg -g [add=gateway,] [remove=gateway,] [list]</td>
<td>Gateway configuration. Allows you to add or remove ICA Gateways.</td>
</tr>
<tr>
<td>ctxbrcfg -m [always</td>
<td>never</td>
</tr>
<tr>
<td>ctxbrcfg -r [set=num,] [list]</td>
<td>Refresh period. Allows you to specify the interval (in minutes) at which the local browser will update the master browser.</td>
</tr>
<tr>
<td>ctxbrcfg -b [set=address</td>
<td>unset</td>
</tr>
<tr>
<td>ctxbrcfg -h</td>
<td>Display usage message.</td>
</tr>
</tbody>
</table>

**Options**

- **-g**: Gateways. Allows you to add or remove ICA Gateways.
- **-m**: Master election. Allows you to influence the criteria used for the master election. **always** makes the local browser try to become the master. **never** instructs the browser to refrain from standing in an election. **neutral** reinstates the default behavior of “no preference.”
- **-r**: Refresh period. Allows you to specify the interval (in minutes) at which the local browser will update the master browser.
- **-b**: Restrict the ICA browser to one subnet. If a XenApp server has more than one network interface card (NIC) and is connected on more than one subnet, configure the server so that the browser listens on only one subnet and ignores broadcasts on the others. Use set to restrict the browser to a subnet. Use unset to remove a restriction. Use list to display current restrictions.
- **-h**: Display usage message.

**Parameters**

- **num**: Specifies the interval (in minutes) at which the local browser will update the master browser.
- **gateway**: Specifies the gateway host name or IP address.
- **address**: The IP address or subnet address to which you want to restrict the browser, in aaa.bbb.ccc.ddd format—that is, 10.20.123.123.

**Remarks**

You must be an administrator to run this command.

If you bind the server to a subnet, make sure that there is only one NIC on this subnet. For more information, see To restrict the ICA browser to a particular subnet or NIC.
See also

ctxqserver—to display information about gateways and the master browser.
ctxcapture

Description

cmp;ctxcapture lets you:

• Capture windows or screen areas and copy them between an application in an ICA
  session window and an application running on the local client device, including
  non-ICCCM-compliant applications.

• Copy graphics between the client device and the X graphics manipulation utility XV. XV
  is a shareware utility that is available for download from the Internet.

tctxcapture is available from the command prompt; it is also available when you connect to
published applications through the ctxwm window manager, if your administrator made it
available, as follows:

• In a seamless window, right click the button in the top, left hand corner of the
  screen to display a menu and choose the Screen Grab option
• In a “full screen” window, right click to display the ctxwm menu and choose the Screen
  Grab option

When ctxcapture starts, a dialog box appears.

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxcapture</td>
</tr>
</tbody>
</table>

See also

cctxgrab—a simple tool to cut and paste graphics from ICA applications to applications
running locally on the client device.
## ctxcfg

**Description**

ctxcfg configures server settings.

### Syntax

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxcfg</td>
<td>-a [ERASE</td>
</tr>
<tr>
<td>ctxcfg</td>
<td>-l [max={UNLIMITED</td>
</tr>
<tr>
<td>ctxcfg</td>
<td>-t [connect={NONE</td>
</tr>
<tr>
<td>ctxcfg</td>
<td>-c [broken={DISCONNECT</td>
</tr>
<tr>
<td>ctxcfg</td>
<td>-p [enable</td>
</tr>
<tr>
<td>ctxcfg</td>
<td>-C [enable</td>
</tr>
<tr>
<td>ctxcfg</td>
<td>-P [set=num</td>
</tr>
<tr>
<td>ctxcfg</td>
<td>-g</td>
</tr>
<tr>
<td>ctxcfg</td>
<td>-e {none</td>
</tr>
<tr>
<td>ctxcfg</td>
<td>-i [INHERIT</td>
</tr>
<tr>
<td>ctxcfg</td>
<td>-s enable [,input={on</td>
</tr>
<tr>
<td>ctxcfg</td>
<td>-D enable,access={ro</td>
</tr>
<tr>
<td>ctxcfg</td>
<td>-k [loadfactor=num]</td>
</tr>
<tr>
<td>ctxcfg</td>
<td>-m [enable</td>
</tr>
<tr>
<td>ctxcfg</td>
<td>-o [set=n]</td>
</tr>
<tr>
<td>ctxcfg</td>
<td>-h</td>
</tr>
</tbody>
</table>

### Options
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td>Allows you to set automatic logon details. Use INHERIT to make the server use logon details specified in the plugin, rather than setting a user name and password for the server using user and pass. Alternatively, you can specify a user name and/or password for all users who log on to the server. Set prompt to TRUE to prompt users for a password, regardless of whether one is specified on the server or the plugin. Use the pass option to prompt users for a logon password. Note that using -g with the list option will not display the password. ERASE erases any user name and password details that were set using the user and pass options and makes the server use logon details specified in the plugin.</td>
</tr>
<tr>
<td>-l</td>
<td>Logons. Allows you to limit the number of users who can be logged on concurrently to the server. Specify an unsigned number or the keyword UNLIMITED to allow an unlimited number of users to log on.</td>
</tr>
<tr>
<td>-t</td>
<td>Timers. Allows you to specify time-out intervals (in minutes) for connected, disconnected, and idle sessions. Only new sessions are affected by changes to the time-out intervals. For example, to specify a time-out interval of 10 minutes for disconnected sessions, use -t disconnect=10. To specify that a timed-out session be logged off rather than reset, use -t disclogoff=num in addition to the -t disconnect setting. Use authentication to specify the maximum duration that a session in the connected state exists on the server, prior to the user logging on or reconnecting. When the specified duration elapses, the session is reset. Use the keyword NONE to disable all time-out settings. Use client check to specify the maximum period of time a client device can be unresponsive before the server checks that the client device is still connected. Use client response to specify the maximum period of time the server waits for a response from a client device before disconnecting sessions automatically. Note: You must configure both client check and client response options to disconnect sessions interrupted by network failure automatically.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **-c** | Connections. Allows you to define how the server handles timed out or broken sessions.  
Set broken to DISCONNECT to disconnect sessions that are broken; set to RESET to terminate broken sessions. Set broken to LOGOFF to log off broken sessions. Logging off sessions allows some applications to exit more cleanly than with RESET. A RESET is performed on the session after 30 seconds if logging off does not fully terminate the session.  
Note: Use the LOGOFF and RESET options with care because users will not be prompted to save their data before sessions are logged off or reset in this way.  
Set reconnect to ORIGINAL to allow reconnection only to a broken or timed out session from the original terminal; set to ANY to allow reconnection to the session from any terminal. |
| **-p** | Client printing. Use to enable or disable client printing. |
| **-C** | Client clipboard. Use to enable or disable the client clipboard. |
| **-P** | Port number. Use to specify a TCP/IP port number on which the server can listen for connections. Use set to use a specific number or reset to use the default number. You must restart the server for the new value to take effect. |
| **-g** | Generate. This generates a list of commands that, if executed, restores all settings to their current values (except the password). You can redirect these commands to a file that you can later execute as a shell script. -g cannot be used with any other argument. |
| **-e** | Encryption. Use to force client devices to use encryption and prevent client devices who do not use encryption from connecting. |
| **-i** | Initial program. Use to specify a program, and path if necessary, to run when the plugin initially connects. INHERIT uses the program and path specified in the plugin. PUBONLY restricts users so that they can connect only to published applications, and prevents users from connecting to the server by name, or to the server desktop. |
| **-s** | Shadowing. Use to enable or disable shadowing. Set input to on to allow the shadower to interact with the shadowed session using the keyboard and mouse. Set notify to on to give users the option to approve or deny the shadowing of their session.  
Note that when enabling shadowing, the default for input is on and the default for notify is on. |
| **-D** | Client drive mapping. Use to enable or disable client drive mapping, where ro is read-only access, and rw is read-write access. When client drive mapping is enabled, it is enabled for all users and all their available local drives. However, you can restrict access using ctxsecurity and ctxmount. |
Switch that allows you to turn features on and off (for example, the ability to log on without a home directory) and set numeric factors (such as the load factor).

To tune the load factor on a server, use `ctxcfg -k loadfactor=num`, where `num` is a load factor value between one and 10000. By default, each server has a load factor of 100.

To allow users whose home directories are unavailable to log on, set `lognohome=1`. To prevent users from logging on without a home directory, set `lognohome=0`.

To allow sessions interrupted by network errors to be automatically reconnected, set `autoreconnect=1`. To prevent sessions interrupted by network errors from being automatically reconnected, set `autoreconnect=0`.

To control the logging of session logons, logoffs, disconnects, and reconnects in the system log file, set `logonlogging`, `logofflogging`, `reconnectlogging`, or `disconnectlogging` to one of the following values: 0 = disable logging. 1 = enable the short form of logging. Provides default syslog information, such as the date and time, and the user name. 2 = enable detailed logging. As above plus the session id, client name, and information about what is running, such as a published application name or desktop. For example, to enable detailed logging of session logons, set `logonlogging=2`.

To prevent any new logons to the server, set `nomorelogons=1`. Users can still reconnect to existing disconnected sessions; but new sessions are not created. To reallow new logons on the server, set `nomorelogons=0`. Note that this value is reset to 0 each time XenApp is restarted.

To disable scrollmouse support, set `disablescrollmouse=1`. All subsequent sessions will not claim this capability.

Mouse-click feedback. Use this option to enable and disable mouse-click feedback. Mouse-click feedback is enabled by default.

You can also configure the thresholds in which mouse-click feedback operates by setting upper and lower threshold values, in milliseconds. The thresholds are like switches that determine when mouse-click feedback is on or off. By default, the upper threshold is 500 milliseconds and the lower threshold is 150 milliseconds.

To display the current settings, use the list option.

Allows you to set the length of delay (in milliseconds) for buffering of graphics. Use `set=n` to specify the delay and reset to reset the current setting to 100ms. To display the current setting, use the list option.

Display usage message.
Remarks

You must be an administrator to run this command.

ctxcfg -t has no effect on anonymous users.

**Caution:** UNIX permissions prevent users from being able to display and access each other’s files. However, if you use ctxcfg -a to allow automatic logon, your users can see directory listings of each others’ files (for example, using the ls command in UNIX) and they can access and display the contents of the files because users are logged on under the same user id. To prevent this, do not use ctxcfg -a with client drive mapping.

See also

ctxanoncfg—to specify an idle time-out period for anonymous users.

ctxsecurity—to restrict access to client drive mapping on a user or group-level basis.

ctxmount—to restrict user access to specific mapped drives.
ctxconnect

Description

ctxconnect lets you connect to a session.

<table>
<thead>
<tr>
<th>Syntax</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxconnect</td>
<td>id</td>
</tr>
<tr>
<td>ctxconnect</td>
<td>-h</td>
</tr>
</tbody>
</table>

Options

- **-h** Display usage message.

Parameters

- **id** Specifies the session id to which to connect.

Remarks

By default, Citrix administrators can connect to any session; other users can connect only to their own sessions.

See also

ctxsecurity—to control which users can connect to other users' sessions.
ctxcreatefarm

ctxcreatefarm is an alias of ctxfarm—see the ctxfarm command for more information.
ctxdisconnect

Description

ctxdisconnect lets you disconnect a session. You can disconnect sessions on the local server or on other servers in the farm.

<table>
<thead>
<tr>
<th>Syntax</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxdisconnect</td>
<td>[ id</td>
</tr>
</tbody>
</table>

Parameters

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Specifies the session id to disconnect.</td>
</tr>
<tr>
<td>servername</td>
<td>Specifies the name of a server in the farm to disconnect. For example, server1:34 means session 34 running on server1.</td>
</tr>
</tbody>
</table>

Remarks

If you do not specify a session id, your own session is disconnected. By default, administrators can disconnect any session; other users can disconnect only their own sessions.

See also

ctxsecurity—to control which users can disconnect other users' sessions.
ctxfarm

Description

ctxfarm lets you create a server farm, join a server to a farm, remove servers from the farm, or change the farm’s passphrase and secret key. XenApp for UNIX uses this secret key to communicate between the servers in the farm.

The ctxcreatefarm and ctxjoinfarm commands are aliases of ctxfarm.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxfarm</td>
<td>-c</td>
</tr>
<tr>
<td>ctxcreatefarm</td>
<td>Create a server farm. Alternatively, use ctxcreatefarm.</td>
</tr>
<tr>
<td>ctxjoinfarm</td>
<td>Join a server to a farm. Alternatively, use ctxjoinfarm.</td>
</tr>
<tr>
<td></td>
<td>Change the farm’s secret key and passphrase.</td>
</tr>
<tr>
<td></td>
<td>Lists servers in a farm and specifies which server is the Management Service Master.</td>
</tr>
<tr>
<td></td>
<td>Remove a server from the farm.</td>
</tr>
</tbody>
</table>

Usage

When you run ctxfarm, ctxcreatefarm, or ctxjoinfarm, you are prompted for, or you can enter, the following information:

| Farm name | If you are creating a farm, specify the name you want to give the farm. |
|-----------| If you are joining a farm, specify the name of the farm you want the server to join. If the server is already in a farm, type the name of the farm you want the server to join and then confirm you want to move the server to the new farm. |
| Farm passphrase | If you are creating a farm, specify a passphrase. This is required by administrators whenever they want to join servers to this farm. |
|            | If you are joining a farm, this is the passphrase specified when the farm was first created. |
|            | If you are changing the secret key and passphrase, specify the new passphrase. The secret key update happens at the same time as the passphrase update. |
Server name

If you are joining a farm, specify the name or IP address of a server already in this farm.

Optionally, if you are removing a server from a farm, you can specify the server you want to remove. If you do not specify a server name, the local server is removed from the farm.

**Remarks**

You must be an administrator to run this command.

The server that you create the farm on will become the Management Service Master, so ensure that you create the farm on an appropriate server.

**Caution:** You must remember the passphrase, because the passphrase you specify when you create the farm is required by administrators whenever they want to join servers to this farm. If you lose the passphrase, you cannot add servers to the farm.

If you update the secret key and passphrase, the command notifies you when the change has been completed successfully. You are also notified of any servers ctxfarm could not reach to update. If ctxfarm cannot contact a reasonable proportion of servers in the farm, the update fails.
ctxgrab

Description

ctxgrab lets you capture dialog boxes or screen areas and copy them from an application in an ICA session window to an application running on the local client device.

ctxgrab is available from a command prompt or, if you are using a published application, from the ctxwm window manager, as follows:

- In a seamless window, right click the button in the top, left hand corner of the screen to display a menu and choose the Screen Grab option
- In a “full screen” window, right click to display the ctxwm menu and choose the Screen Grab option

When ctxgrab starts, a dialog box appears.

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxgrab</td>
</tr>
</tbody>
</table>

See also

ctxcapture—a more extensive tool that lets you cut and paste graphics between ICA applications and applications running on the client device.
ctxjoinfarm

cctxjoinfarm is an alias of ctxfarm—see the ctxfarm command for more information.
ctxlogoff

Description
ctxlogoff logs off a user from a XenApp server. You can log off sessions on the local server or on other servers in the farm.

<table>
<thead>
<tr>
<th>Syntax</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxlogoff</td>
<td>[servername:id</td>
</tr>
<tr>
<td>ctxlogoff</td>
<td>-h</td>
</tr>
</tbody>
</table>

Options
-h Display usage message.

Parameters
id Specifies the session id to log off.
servername:id Specifies the session id to log off on a particular server, where servername is the name of a server in the farm. For example, server1:34 means session 34 running on server1.

Remarks
If a user is not specified, you are logged off.

By default, administrators can log off any user; other users can log off only themselves.

See also
ctxsecurity—to control which users can log off other users’ sessions.
ctxlpr

Description

ctxlpr prints to a client printer.

Syntax

ctxlpr [-P printerName] [-b] [-n] [file1, …file10]

Options

-P  Print a file to a printer (or printer port) other than the default. This is the printer name or printer port shown in the first column of the output from ctxprinters.

-b  Print the job in the background.

-n  Only one print job can be handled at a time in any one session. If a call is made to ctxlpr while a previous job is still printing, the default behavior is for the second command to wait for the first job to end before continuing. Use the -n option to cause a second print job to fail rather than wait. Use this to stop applications from waiting while other printer jobs are handled.

-h  Display usage message.

Parameters

file  Specifies the name of a file to print. Up to 10 files can be specified; each file is treated as a separate print job. If no files are specified, ctxlpr takes its input from standard input (stdin).

printerName  Name of the printer (or printer port) other than the default.

See also

ctxprinters—to list printers installed on the client device.
**ctxlsdcfg**

**Description**

ctxlsdcfg configures communication with the license server.

You can run this command interactively or non-interactively. Use the ctxlsdcfg command to configure communication with the license server interactively, using the `License Config>` command prompt. Use the ctxlsdcfg command with the required options to configure communication with the license server non-interactively.

**Syntax**

<table>
<thead>
<tr>
<th>Command</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxlsdcfg</td>
<td>-s server_name</td>
</tr>
<tr>
<td>ctxlsdcfg</td>
<td>-p port_number</td>
</tr>
<tr>
<td>ctxlsdcfg</td>
<td>-e edition</td>
</tr>
<tr>
<td>ctxlsdcfg</td>
<td>-c compatibilty</td>
</tr>
<tr>
<td>ctxlsdcfg</td>
<td>-m mode</td>
</tr>
<tr>
<td>ctxlsdcfg</td>
<td>-h</td>
</tr>
</tbody>
</table>

**Options**

- **-s** Specify the name of the license server.
- **-p** Specify the port number of the license server.
- **-e** Specify the current product edition (either Enterprise or Platinum).
- **-c** Specify whether XenApp for UNIX can share licenses with servers running Citrix Presentation Server 4.0 or earlier, or with servers running Citrix Presentation Server 4.5 or later (either 4.0 or post4.0).
- **-m** Specify whether XenApp runs in feature pack or base mode (either FeaturePack1 or Base).
- **-h** Display usage message.

**Usage**

When you run the ctxlsdcfg command interactively, the `License Config>` command prompt appears and you can enter the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list</td>
<td>Display the current license server name, port number, and product edition.</td>
</tr>
<tr>
<td>server server_name</td>
<td>Specify the name of the license server.</td>
</tr>
<tr>
<td>port port_number</td>
<td>Specify the port number of the license server.</td>
</tr>
</tbody>
</table>
**ctxlsdcfg**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>edition</strong></td>
<td>Specify the current product edition (either Enterprise or Platinum).</td>
</tr>
<tr>
<td><strong>compatibility</strong></td>
<td>Specify whether XenApp for UNIX can share licenses with servers running Citrix Presentation Server 4.0 or earlier, or with servers running Citrix Presentation Server 4.5 or later (either 4.0 or post4.0).</td>
</tr>
<tr>
<td><strong>mode</strong></td>
<td>Specify whether XenApp runs in feature pack or base mode (either FeaturePack1or Base).</td>
</tr>
<tr>
<td><strong>exit</strong></td>
<td>Exit the program.</td>
</tr>
</tbody>
</table>

**Remarks**

You must be an administrator to run this command.

Settings for compatibility and mode options are propagated to all servers in the farm only if Citrix XenApp 4.0, with Feature Pack 1, for UNIX is installed on the Management Service Master server.
ctxmaster

Description

ctxmaster shows the master ICA browser address.

<table>
<thead>
<tr>
<th>Syntax</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxmaster</td>
<td>[-h]</td>
</tr>
</tbody>
</table>

Options

| -h | Display usage message. |

Remarks

Citrix recommends you use the ctxqserver -master command instead to display the server acting as the master browser.

See also

ctxqserver—to display the master browser address.
ctxmount

Description

tctxmount configures user access to specific mapped drives.

When you enable client drive mapping using ctxcfg, all the local drives available to a user are mapped. However, you can configure access to particular mapped drives using the ctxmount command. You can do this for particular users or for every user who connects to a XenApp server.

To use the ctxmount command, you modify it within the ctxsession.sh script.

<table>
<thead>
<tr>
<th>Syntax</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxmount</td>
<td>[ -d</td>
</tr>
</tbody>
</table>

Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>Disconnect a drive.</td>
</tr>
<tr>
<td>-ro</td>
<td>Configure access to a drive as read-only. If you specify a currently connected drive, this drive is made read-only.</td>
</tr>
</tbody>
</table>

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>drivelist</td>
<td>Specify the drive letters to which you want to configure access (A B C ... Z) or all to specify all available drives. If you do not specify a drivelist, the default of all is used.</td>
</tr>
</tbody>
</table>

Remarks

Settings configured using ctxcfg take precedence over any settings configured using ctxmount. For example, if you enable read-only access to mapped drives using ctxcfg, read-write access cannot be granted using ctxmount.

See also

ctxcfg—to enable or disable client drive mapping for all users and all available local drives.

ctxsecurity—to restrict access to client drive mapping on a user or group level basis.
ctxmsg

Description

ctxmsg sends a message to a particular session or to all sessions, either on the local server or in the entire server farm.

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxmsg [-w] {id</td>
</tr>
<tr>
<td>ctxmsg -a message</td>
</tr>
<tr>
<td>ctxmsg -s servername message</td>
</tr>
<tr>
<td>ctxmsg -S message</td>
</tr>
<tr>
<td>ctxmsg -h</td>
</tr>
</tbody>
</table>

Options

- **-w**
  Suspends the ctxmsg program until the message either times out or the user dismisses it. That is, the command prompt returns only when the user responds or the message times out.

- **-a**
  Send a message to all users on the local server.

- **-s**
  Send a message to all users on a particular server.

- **-S**
  Send a message to all users on all servers in the farm.

- **-h**
  Display usage message.

Parameters

- **id**
  Session id of the user to whom you want to send the message.

- **servername**
  Name of a server in the farm. For example, server1:34 means session 34 running on server1.

- **message**
  The text you want to send. To send a message that contains spaces, enclose it within double quotes.

- **timeout**
  Specify a time-out (in seconds) for the message. If no time-out is specified, or the time-out is specified to be zero, the message dialog box remains displayed until dismissed by the user.

See also

cctxquser or ctxqsession—to display users’ session IDs.

cctxsecurity—to control which users can send messages to other users’ sessions.

cctxshutdown—to inform users that the server is about to shut down.
ctxprinters

Description

ctxprinters lists printers installed on the client device and indicates which is the default.

For each printer, the list displays:

- The printer name or printer port (for example, lpt1). You can use this in the ctxlpr -P command to specify a printer other than the default.
- The name of the device driver.
- The name of the port to which the printer is attached.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxprinters</td>
<td>-h</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Options</th>
<th>Display usage message.</th>
</tr>
</thead>
</table>

See also

ctxlpr—to print to a client printer.
ctxqserver displays information about XenApp servers on the network.

**Note:** Some options, such as -license, display information only for servers running versions prior to Version 4.0 that use the previous licensing method. For information about the new Citrix Licensing method, see *Getting Started with Citrix Licensing*.

### Syntax

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxqserver</td>
<td>[server_name]</td>
</tr>
<tr>
<td>ctxqserver -addr</td>
<td>server_name</td>
</tr>
<tr>
<td>ctxqserver -app</td>
<td>[application_name</td>
</tr>
<tr>
<td>ctxqserver -disc</td>
<td>[application_name</td>
</tr>
<tr>
<td>ctxqserver -gateway</td>
<td>[server_name]</td>
</tr>
<tr>
<td>ctxqserver -gatewaylicense:</td>
<td>IP_address</td>
</tr>
<tr>
<td>ctxqserver -license</td>
<td>[server_name]</td>
</tr>
<tr>
<td>ctxqserver -load</td>
<td>server_name</td>
</tr>
<tr>
<td>ctxqserver -master</td>
<td></td>
</tr>
<tr>
<td>ctxqserver -netlicense</td>
<td></td>
</tr>
<tr>
<td>ctxqserver -ping</td>
<td>[-count:value] [-size: value] server_name</td>
</tr>
<tr>
<td>ctxqserver -reset</td>
<td>server_name</td>
</tr>
<tr>
<td>ctxqserver -serial</td>
<td>[server_name]</td>
</tr>
<tr>
<td>ctxqserver -stats</td>
<td>server_name</td>
</tr>
<tr>
<td>ctxqserver -tcpserver:x</td>
<td></td>
</tr>
<tr>
<td>ctxqserver -h</td>
<td></td>
</tr>
</tbody>
</table>

### Options

- **-addr** Display the network address of a specific server.
- **-app** List all published applications and the server load. Specify the name of an application or server to narrow the list.
- **-disc** List all disconnected sessions. Specify the name of an application or client device to narrow the list.
- **-gateway** List the ICA gateways known to each server. Specify a server name to narrow the list.
- **-gatewaylicense** Display the number of remote licenses available from a gateway. Specify the IP address of the gateway; that is, ctxqserver -gatewaylicense:12.12.123.12.
**-license** List the licenses on each server. Mach displays the number of licenses kept local to the server; Pool displays the number of pooled licenses; Total shows the sum of the local and pooled licenses.

Specify a server name to narrow the list.

**-load** Display the loading for a particular server.

**-master** Display the IP address of the master browser.

**-netlicense** Display information about the number of licenses installed and in use on the local network. The number of licenses kept local to the server and the number pooled is also shown.

**-ping** Ping the named server.

**-reset** Reset statistics about the activities of the browser (for example, elections sent/received, packets sent/received) for the named server.

**-serial** Display the licenses on each server. Specify a server name to narrow the list.

**-stats** Display statistics about the activities of the browser for a particular server.

**-tcpserver:** Sets the TCP/IP default server address to x.

**-h** Display usage message.

### Parameters

<table>
<thead>
<tr>
<th>server_name</th>
<th>Name of a specific server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>application_name</td>
<td>Name of a published application.</td>
</tr>
<tr>
<td>-count:value</td>
<td>Use with the ping option to specify the number of packets to send. The default is five packets.</td>
</tr>
<tr>
<td>-size:value</td>
<td>Use with the ping option to specify the packet size. The default is 256 bytes.</td>
</tr>
<tr>
<td>IP_address</td>
<td>TCP/IP address of a server.</td>
</tr>
</tbody>
</table>
**ctxqsession**

**Description**

ctxqsession displays a default listing of session details.

ctxqsession displays information about ICA connections to the local server, another server in the farm, or the entire server farm. The information includes, where appropriate, user name, session ID, state, type, and device.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxqsession</td>
<td>[-s servername]</td>
</tr>
<tr>
<td>ctxqsession</td>
<td>-S</td>
</tr>
<tr>
<td>ctxqsession</td>
<td>-h</td>
</tr>
</tbody>
</table>

**Options**

- `-s`       Display information about a particular server.
- `-S`       Display information about all servers in the farm.
- `-h`       Display usage message.

**Parameters**

- `servername`       Name of a specific server.

**See also**

ctxquser—to display session user details.

ctxquery—to display additional session details or details in a different format.
ctxquery

Description

ctxquery allows you to display a comprehensive list of session details and to configure the display of these details.

ctxquery displays information about connections to one or more XenApp servers in a farm. This includes information about users, sessions, client devices, servers, and published applications. You can also use ctxquery to produce machine-readable output.

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxquery</td>
</tr>
<tr>
<td>ctxquery</td>
</tr>
<tr>
<td>ctxquery</td>
</tr>
<tr>
<td>ctxquery</td>
</tr>
<tr>
<td>ctxquery</td>
</tr>
</tbody>
</table>

Options

- **-f** Configure the display format using characters to indicate the information that should be shown.
- **-o** Configure the display format using keywords to indicate the information that should be shown.
- **-m** Produce machine-readable output. Spaces are removed from column headers so that a constant number of columns is displayed on every line.
- **-s** Display information about a particular server.
- **-S** Display information about all servers in the farm.
- **-h** Display usage message.

Parameters

**short_format_options** Characters that indicate the information you want to display. See the following table for details.

**long_format_options** Keywords that indicate the information you want to display. See the following table for details.

**servername** Name of a specific server.

**user username** Name of a particular user you want to query

<table>
<thead>
<tr>
<th>Long Format Options</th>
<th>Short Format Options</th>
<th>Description</th>
</tr>
</thead>
</table>


<table>
<thead>
<tr>
<th>Field</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>addr</td>
<td>a</td>
<td>Client address. The hardware address of the client device.</td>
</tr>
<tr>
<td>app</td>
<td>p</td>
<td>Published application name.</td>
</tr>
<tr>
<td>dev</td>
<td>d</td>
<td>Client device name.</td>
</tr>
<tr>
<td>id</td>
<td>i</td>
<td>Session ID. This is in the format <code>servername:id</code>, where <code>servername</code> is the name of a server in the farm, and <code>id</code> is the session identifier.</td>
</tr>
<tr>
<td>idle</td>
<td>I</td>
<td>Idle time. The length of time since there was user activity in this session. It may take some time to display this, depending on the number of users and how they are distributed across servers.</td>
</tr>
<tr>
<td>logon</td>
<td>l</td>
<td>Logon time. The time the user logged on to the system.</td>
</tr>
<tr>
<td>sess</td>
<td>n</td>
<td>Session name; for example: tcp#41.</td>
</tr>
<tr>
<td>sess#</td>
<td>N</td>
<td>Session number only. Use to display the session number without the “<code>servername:</code>” prefix.</td>
</tr>
<tr>
<td>srvr</td>
<td>s</td>
<td>Server name. The name of a server in the farm.</td>
</tr>
<tr>
<td>state</td>
<td>S</td>
<td>Session state:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- listen - indicates the session that is listening for new incoming connections.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- active - indicates an established, active connection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- connq - indicates a brief session initialization phase that occurs before the logon prompt appears and during reconnect.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- init - a brief session initialization phase.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- conn - indicates a session that is being connected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- disc - indicates a disconnected session.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- down - indicates a broken session.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- shadow - indicates that the user of this session is shadowing another.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- reset - indicates a session currently being reset.</td>
</tr>
<tr>
<td>type</td>
<td>t</td>
<td>Session type. <code>wdica</code> indicates that the ICA protocol is being used.</td>
</tr>
<tr>
<td>user</td>
<td>u</td>
<td>User name.</td>
</tr>
<tr>
<td>xdp</td>
<td>x</td>
<td>X display number.</td>
</tr>
<tr>
<td>Xdp</td>
<td>X</td>
<td>X display number, without the leading colon (:)</td>
</tr>
</tbody>
</table>
See also

ctxqsession—to display a default list of session details.

ctxquser—to display a default list of session user details.
ctxquser

Description

ctxquser displays a default listing of session user details.

ctxquser displays information about users logged on to the local server, another server in the farm, or the entire server farm. The information displayed includes the user name, the session ID, the state, the time the user has been idle, and the total time the user has been logged on.

Syntax

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxquser</td>
</tr>
<tr>
<td>ctxquser [user username]</td>
</tr>
<tr>
<td>ctxquser -s servername [user username]</td>
</tr>
<tr>
<td>ctxquser -S [user username]</td>
</tr>
<tr>
<td>ctxquser -h</td>
</tr>
</tbody>
</table>

Options

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s</td>
<td>Display information about a particular server.</td>
</tr>
<tr>
<td>-S</td>
<td>Display information about all servers in the farm.</td>
</tr>
<tr>
<td>-h</td>
<td>Display usage message.</td>
</tr>
</tbody>
</table>

Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>servername</td>
<td>Name of a specific server.</td>
</tr>
<tr>
<td>user username</td>
<td>Name of a particular user you want to query.</td>
</tr>
</tbody>
</table>

See also

ctxqsession—to display session details.

ctxquery—to display additional session details or details in a different format.
ctxreset

Description

ctxreset resets a session.

ctxreset resets an ICA connection on the local server or another server in the farm. You specify the session to be reset using its session id.

Syntax

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
</table>
| ctxreset \{id | servername:id \} | \n
<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxreset -h</td>
<td>Display usage message.</td>
</tr>
</tbody>
</table>

Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Session id of the session you want to reset.</td>
</tr>
<tr>
<td>servername</td>
<td>Name of a server in the farm. For example, server1:34 means session 34 running on server1.</td>
</tr>
<tr>
<td>-h</td>
<td>Display usage message.</td>
</tr>
</tbody>
</table>

Remarks

By default, administrators can reset any session; other users can reset only their own sessions.

See also

ctxqsession—to display the current sessions.

ctxquser—to display session user details.

ctxsecurity—to control which users can use ctxreset to reset other users’ sessions.
ctxsecurity

Description

ctxsecurity configures XenApp security.

XenApp security controls a user’s access to commands and sessions. When you install XenApp, default security settings are applied that automatically control access at a global level to XenApp-secured functions. Security can also be controlled at user and group levels.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxsecurity secured_function -l</td>
<td>Display security settings for a particular secured function.</td>
</tr>
<tr>
<td>ctxsecurity secured_function -a {allow</td>
<td>deny}</td>
</tr>
<tr>
<td>ctxsecurity secured_function -u {user_name} {allow</td>
<td>deny}</td>
</tr>
<tr>
<td>ctxsecurity secured_function -g {group_name} {allow</td>
<td>deny}</td>
</tr>
<tr>
<td>ctxsecurity secured_function {-u user_name</td>
<td>-g group_name} inherit</td>
</tr>
</tbody>
</table>

Options

- **-l**  
  Display security settings for a particular secured function.

- **-a**  
  Change the global security setting for a secured function.

- **-u**  
  Change security at user level for a secured function.

- **-g**  
  Change security at group level for a secured function.

- **-h**  
  Display usage message.

Parameters

- **secured_function**  
  A particular tool; for example, shadow. The secured functions are shown in the following table.

- **allow**  
  Permit access to the secured function.

- **deny**  
  Prevent access to the secured function.

- **user_name**  
  User account name.

- **group_name**  
  Group name to which the user belongs.

- **inherit**  
  Remove previous user or group security settings and inherit settings from the level above.

Secured Functions

The following table lists the secured functions together with their default settings after installation.

<table>
<thead>
<tr>
<th>Secured Function</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>shadow</td>
<td>default</td>
</tr>
<tr>
<td>Secured function</td>
<td>XenApp security determines</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>login</td>
<td>Which users can log on to the server.</td>
</tr>
</tbody>
</table>
| sendmsg (ctxmsg) | Which users can use ctxmsg to send messages to other users’ sessions. | Allow  
|                  | Deny for anonymous users | |
| connect (ctxconnect) | Which users can use ctxconnect to connect to other users’ sessions. | Deny |
| disconnect (ctxdisconnect) | Which users can use ctxdisconnect to disconnect other users’ sessions. | Deny |
| logoff (ctxlogoff) | Which users can use ctxlogoff to log off other users’ sessions. | Deny |
| reset (ctxreset) | Which users can use ctxreset to reset other users’ sessions. | Deny |
| shadow (ctxshadow) | Which users can use ctxshadow to shadow other users’ sessions. | Allow  
|                  | Deny for anonymous users | |
| cdm              | Which users can use client drive mapping to access their local drives. | Allow |

**Remarks**

You must be an administrator to run this command.

**See also**

cctxcfg—to enable and disable shadowing and client drive mapping.
ctxshadow

Description

ctxshadow starts a shadowing session. Shadowing lets you monitor and interact with another active session.

The session that issues the ctxshadow command is referred to as the shadower, and the session being shadowed is called the shadowed session.

Syntax

ctxshadow {id | servername:id} [-v] [-h[a][c][s]+]x

Options

-v
Verbose output. Displays additional information.

-h
Use with a session id to configure a hotkey combination to end shadowing; for example, ctxshadow id [-h[[a][c][s]+]x] —Or— Specify ctxshadow -h to display a usage message.

Parameters

id —Or— servername:id
Specify the session to be shadowed using its session ID. Alternatively, specify the local server name and ID; for example, server1:34 means session 34 running on server1. Note that you cannot shadow a session on another server.

{a|c|s}+x
Specify the hotkey combination you want to use to end shadowing. Choose this combination from:

a | c | s where a = ALT; c = CTRL; s = SHIFT x where x is an alphanumeric character (a to z and 0 to 9)

Note: You can use any combination of a, c, and s, including all or none. For example, to begin shadowing and to specify a hotkey combination of ALT and q to stop shadowing, type: ctxshadow {id | name} -h a+q

To End a Shadowing Session

By default, you can end shadowing by holding down the CTRL key and pressing the asterisk (*) key on your keyboard’s numeric keypad. However, if you cannot use this hotkey combination or you prefer to use an alternative, you can configure a different combination using the -h option.
Remarks

Note that virtual channel data (instructions to the server that affect only the shadowed session) is not shadowed. For example, if you print a file while shadowing a session, the file is queued at the shadowed session’s printer.

You may also get some unexpected results using the clipboard channel. The user of the shadowed session can use the clipboard to copy and paste between the ICA session and applications running locally. As shadower, you cannot access the contents of the shadowed session’s clipboard—information in the clipboard belongs to the shadowed session. However, if you copy information to the clipboard while shadowing, this information is available to the shadowed session for pasting.

See also

ctxcfg—for shadowing configuration at the server.
ctxquser or ctxqsession—to display session ID.
ctxsecurity—to control which users can shadow other users’ sessions.
ctxshutdown

Description

ctxshutdown stops the XenApp processes.

Syntax

txshutdown [-q] [-m seconds] [-l seconds] [message]

txshutdown -h

Options

-q
Quiet mode. Use to reduce the amount of information displayed to the administrator by the ctxshutdown command.

-m
Specify when the shut down process will begin, and how long the message will appear, in seconds. The default is 60 seconds. When this period expires and the shut down process begins, applications that have registered “window hints” (the WM_DELETE_WINDOW attribute) will attempt to interactively log the user off. Applications that have not registered “window hints” will terminate immediately.

-l
Specify how long applications that have registered “window hints” have to interactively log users off. The default is 30 seconds. When this period expires, any remaining sessions are terminated automatically, users are logged off automatically, and the XenApp process stops.

-h
Display usage message.

Parameters

message
Specify the message displayed to all users logged on to the server. If you do not specify a message, the default message “Server shutting down. Auto logoff in x seconds” appears, where x = the number of seconds specified in the -m option (or the default of 60 seconds if this is not specified).

Remarks

You must be an administrator to run this command.

See also

ctxsrv—to stop the XenApp processes on a server.
ctxsrv

Description

ctxsrv starts up or stops the server processes.

You can use ctxsrv to start up and stop all the processes on the server, or to start up and stop an individual process, such as the ICA browser or SSL Relay.

<table>
<thead>
<tr>
<th>Syntax</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxsrv</td>
<td>start [browser</td>
</tr>
<tr>
<td>ctxsrv</td>
<td>stop [browser</td>
</tr>
<tr>
<td>ctxsrv</td>
<td>-h</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Options</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>browser</td>
<td>The Citrix ICA Browser Service.</td>
</tr>
<tr>
<td>sslrelay</td>
<td>SSL Relay.</td>
</tr>
<tr>
<td>cdm</td>
<td>Client drive mapping. If you stop client drive mapping using ctxsrv stop, this immediately stops the client drive mapping process on the server, and disables client drive mapping for all connections, including any existing connections.</td>
</tr>
<tr>
<td>lsd</td>
<td>License Service daemon.</td>
</tr>
<tr>
<td>msd</td>
<td>Management Service daemon.</td>
</tr>
<tr>
<td>server</td>
<td>The connection server.</td>
</tr>
<tr>
<td>all</td>
<td>All server processes.</td>
</tr>
<tr>
<td>-h</td>
<td>Display usage message.</td>
</tr>
</tbody>
</table>

Remarks

Citrix recommends you use the ctxshutdown command to stop the XenApp processes on a server. If you use ctxsrv to stop XenApp, and sessions are still active when the server is stopped, the sessions are terminated and unsaved applications or user data can be lost.

You must be root or an administrator to run this command.

Do not run the commands ctxsrv start all, ctxsrv stop all, ctxsrv start cdm and ctxsrv stop cdm from within the /ctxmnt directory, or the client drive mapping process fails.

See also

ctxshutdown—to shut down the processes on a server.
ctxcfg—to disable client drive mapping for new connections only.
### XML Service Commands

The XML Service commands are as follows:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxnfusesrv</td>
<td>configure the Citrix XML Service HTTP port, enable publishing mode, DNS address resolution, and specify the SSL Relay port</td>
</tr>
</tbody>
</table>
ctxnfusesrv

Description

ctxnfusesrv configures the server listening port, or lists the current listening port. ctxnfusesrv can also be used to enable users to make secure connections using SSL and to enable and disable DNS address resolution.

Syntax

ctxnfusesrv
{ -l | -port portnumber}

ctxnfusesrv
-ssl-port portnumber

ctxnfusesrv
-dns [ enable | disable ]

ctxnfusesrv
-bind { all | subnet-address [subnet-mask]}

Options

- port
  Configures the HTTP server listening port. The default port number is 80.

- l
  Lists the current HTTP server listening port, the publishing mode, the SSL port number, and the DNS address resolution setting.

- ssl-port
  Specifies the port number on which SSL Relay listens for connections (this is the SSL port you configured using the SSL Relay configuration tools). You need to run this command only if you are not using TCP port 443, which is the standard port for SSL-secured communications.

- dns
  Enables and disables Domain Name System (DNS) address resolution. By default, DNS is disabled and XenApp servers reply to browsing requests with an IP address.

- bind
  Restricts ICA master browser broadcasts made by the XML Service to one subnet. If the server has more than one network interface and is connected to more than one network or subnet, this option configures the network to which ICA master browser broadcasts are sent. If the network is subnetted, the appropriate subnet network mask must be specified. By default, ICA master browser requests are broadcast locally on all available interfaces.

Parameters

portnumber
TCP port number.

enable
Enables DNS address resolution.

disable
Disables DNS address resolution.

subnet-address
Specifies the subnet or interface address to which ICA master browser broadcasts are sent. The format of the subnet address is aaa.bbb.ccc.ddd; for example, 10.20.131.123.
subnet-mask

| subnet-mask | Specifies the netmask corresponding to the subnet address. The format of the subnet mask is aaa.bbb.ccc.ddd; for example, 255.255.240.0. |

Remarks

You must be an administrator to run this command.

If you make changes using ctxnfusesrv -port, you must stop and restart the XML Service using ctxsrv {start | stop} msd for the changes to take effect.

See also

ctxsrv—to start and stop the XML Service.
SSL Relay for UNIX Administration

This section of the library provides up-to-date product information about SSL Relay for UNIX, which is a component of Citrix XenApp for UNIX. The section is for system administrators who are responsible for installing, configuring, and maintaining SSL Relay, Citrix XenApp for UNIX, and the Web Interface.

These topics assume you have knowledge of:

- Citrix XenApp for UNIX
- Citrix XML Service for XenApp for UNIX
- Web Interface

<table>
<thead>
<tr>
<th>Features of SSL Relay</th>
<th>Installing a Server Certificate on a Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of Security, SSL, and Cryptography</td>
<td>Configuring SSL Relay Ready for Use</td>
</tr>
<tr>
<td>Planning Your SSL Relay Deployment</td>
<td>Changing the SSL Relay Configuration</td>
</tr>
<tr>
<td>Generating or Renewing a Certificate</td>
<td>Managing Your Server Certificates</td>
</tr>
</tbody>
</table>
Introducing SSL Relay

SSL Relay provides the ability to secure data communications using the Secure Sockets Layer (SSL) protocol. SSL provides server authentication, encryption of the data stream, and message integrity checks.

You can use SSL Relay to secure communications:

- In a Web Interface deployment, between the Web server and the XenApp server.
- Between an SSL-enabled plugin and a XenApp server.

In a Web Interface Deployment

If you enable SSL on a server running the Web Interface and SSL Relay on a XenApp server, the data passed between the Web server and XenApp is secured using SSL encryption. SSL Relay uses a TCP port to listen for SSL-secured connections. When it receives a connection, it decrypts the data before redirecting the data to the Citrix XML Service.

Between an SSL-enabled Plugin and a XenApp Server

If you enable SSL Relay on a XenApp server and deploy SSL-enabled plugins, data passed between the client device and the XenApp server is encrypted using SSL. SSL Relay uses a TCP port to listen for SSL-secured connections. When it receives an SSL connection, it decrypts the data before redirecting the data to the server or, if the plugin selected SSL+HTTPS browsing, to the Citrix XML Service.

The following diagram shows how you can use SSL Relay to secure communications at various points in your Citrix installation.
SSL Relay for UNIX is included automatically when you install Citrix XenApp for UNIX.

Before you can begin using SSL Relay, you must plan how to use SSL to secure communications in your XenApp installation, obtain digital certificates, and configure the SSL Relay. These steps are described in this manual.

If you are unfamiliar with the SSL protocol and the concepts of cryptography on which SSL is based, we recommend that you read the section "Overview of Security, SSL, and Cryptography".

**SSL Relay Features**

This section describes the key features and benefits of using Citrix XenApp SSL Relay for UNIX.

**Encryption of the data stream**—SSL encrypts information to ensure its confidentiality and to prevent eavesdropping. One of the main benefits of using SSL to secure communications is that it allows you to choose the type of encryption you want to use. SSL Relay supports a range of encryption types. You choose the type of encryption you want to use by selecting a *ciphersuite*. A ciphersuite defines the cipher algorithm and parameters to be used, such as the size of the keys.

**Authentication of the server**—using SSL, users can verify the identity of a XenApp server. This guards against the possibility of a third party masquerading as the intended recipient. Some of the checks that the plugin performs include:
Introducing SSL Relay

- A check for the root certificate. If there is no root certificate, the connection fails.
- A check that the root certificate has not expired.

SSL Relay and SSL-enabled plugins do not perform certificate revocation checking.

**Message integrity checks**—SSL ensures that the contents of a message remains intact until it reaches its intended destination. This prevents accidental or intentional data manipulation.

**Special account for SSL Relay administration**—SSL Relay requires you to create a special user account for SSL administration, called the ctxssl user. The ctxssl user is part of the Citrix server administrator group account ctxadm. Only the ctxssl user can run the SSL Relay commands and access the SSL Relay directories and files. For information about creating this account, see the *Citrix XenApp for UNIX Administrator’s Guide*.

**Support for VeriSign and Baltimore root certificates**—support for VeriSign and Baltimore root certificates is already built into SSL-enabled plugins and servers running the Web Interface. Therefore, there is no need to obtain and install root certificates on the client device or on the server running the Web Interface if you are using these Certificate Authorities. In addition to this support, SSL Relay enables you to add additional root certificates, for example, from an in-house authority.

**Tool for generating certificate requests**—SSL Relay includes the certificate request generation utility ctxcertreq that creates a certificate request file that you can send to a CA. The utility prompts you for the required information and generates a private/public key pair, and a certificate signing request for verification by the CA.
Overview of Security, SSL, and Cryptography

This section is intended for users who are unfamiliar with SSL and the concepts of cryptography on which SSL is based. The section discusses what the main threats to secure communications are and how SSL is designed to tackle these threats. Also discussed are the differences between SSL and Citrix SecureICA Services.
With Citrix XenApp and the Web Interface, you can instantly extend the reach of any application to any user, using any device in any location, regardless of client device hardware or network connectivity. However, with this ability there is the concern of how you safeguard the security of data transmission between devices.

The three main types of threat to secure communications are: eavesdropping, misrouting, and data manipulation. The following describes these threats in the context of a XenApp and Web Interface installation.

**Eavesdropping**

The contents of a message may be read as it is transmitted over a network. Eavesdropping on sensitive information, such as user ids and passwords, is therefore a serious threat to security.

For example, during communication between a client device and a XenApp server, user login credentials are transmitted. The credentials are encrypted, but the encryption strength depends on the settings in the plugin. If an attacker can crack the binary ICA protocol, they can eavesdrop on this information and use it to gain unauthorized access to the server.

**Misrouting**

A message could, in theory, be intercepted along its path and re-routed to an unauthorized user or a counterfeit server.

For example, in a Web Interface deployment, user credentials and application set information is passed between the Java objects on the Web server and the Citrix XML Service on the XenApp server. In a typical Web Interface session, the Java objects pass credentials to the XML Service for user authentication and the XML Service returns application set information. The Web server and server farm use a TCP/IP connection and the Web Interface XML protocol to pass the information.

The Web Interface XML protocol uses clear text to exchange all data with the exception of passwords, which it passes using Basic encryption. The XML communication is therefore vulnerable to attack. An attacker can impersonate the XenApp server and intercept authentication requests.

**Data Manipulation**

The contents of a message might be deliberately modified or corrupted as it travels along its path.
For example, during Web Interface communication, data is passed between the Web browser on the client device and the Web server. An attacker may intercept and modify this data.
Using SSL to Tackle Security Threats

The following describes how SSL counteracts the threats to secure communications by providing three types of security control: authentication, confidentiality, and integrity.

### Authentication

SSL addresses the threat of misrouting by providing authentication of the XenApp server. With SSL, users can verify the true identity of a server or Web site. This guards against the possible misrouting of a message.

### Confidentiality

SSL addresses the threat of eavesdropping by ensuring the confidentiality of information as it traverses a network. SSL prevents possible eavesdropping by creating a secure connection over which the user can pass their credentials and data. The connection is secure because it is encrypted using negotiated keys, to which a third party cannot gain access.

### Integrity

SSL addresses the threat of data manipulation by ensuring the integrity of information. Using SSL you can prevent accidental or intentional data manipulation by ensuring that the contents of a message remain intact as it traverses the network, until it reaches its intended destination.
Comparing SSL with Citrix SecureICA

Using Citrix SecureICA Services, you can encrypt the information sent between a XenApp server and a client device. This makes it virtually impossible for unauthorized users to open an encrypted transmission and, in the unlikely event that an attack succeeded, SecureICA ensures that the attacker only sees meaningless screen commands and not sensitive information.

Therefore, Citrix SecureICA Services provides confidentiality to guard against the threat of eavesdropping. However, as the previous discussion shows, there are other security risks and using encryption is only one aspect of a comprehensive security policy.

Unlike SSL, SecureICA does not provide authentication of the XenApp server, therefore information could, in theory, be intercepted as it crosses the network and re-routed to a counterfeit server. Also, SecureICA does not provide integrity checking.

**Note:** Citrix SecureICA is not available for XenApp for UNIX servers.
About Cryptography

SSL uses cryptography to secure communications. Cryptography provides the ability to encode messages to ensure confidentiality. Cryptography is also used to authenticate the identity of a message and to ensure the integrity of its contents.

A message is sent using a secret code, called a cipher. The cipher scrambles the message so that it cannot be understood by anyone other than the sender and receiver. Only the receiver who has the secret code can decipher the original message, thus ensuring confidentiality.

Cryptography also allows the sender to include special information in the message that only the sender and receiver know. When the receiver sees this special information, they know that the message is authentic.

Cryptography also ensures that the contents of a message have not been altered. To do this, the sender includes a cryptographic operation called a hash function in the message. A hash function is a mathematical representation of the information, similar to the checksums found in communication protocols. The sender also includes a secret value, known only to the sender and receiver. When the message arrives at its destination, the receiver calculates the hash function. If the receiver’s hash function value is the same as the sender’s, then the integrity of the message is assured.

Types of Cryptography

There are two main types of cryptography:

- Secret key cryptography
- Public key cryptography

The following section describes how these types of cryptography work and why they are often combined, as in SSL.

Secret key cryptography. Secret key cryptography is also known as Symmetric Key Cryptography. With this type of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are scrambled by the sender using the key, and unscrambled by the receiver using the same key. This method works well if you are communicating with only a limited number of people, but it becomes impractical to exchange secret keys with large numbers of people. And there is also the problem of how you communicate the secret key securely.

Public key cryptography. Public key cryptography is also known also as Asymmetric Key Cryptography. With this type of cryptography, one key is used to scramble the message and another key is used to unscramble it. There are always two keys: a public key and a private key. The public key is made available to everyone, while the private key is kept secret. Messages scrambled with one key can only be unscrambled using the other key. The following example illustrates how public key cryptography works:
1. Phil wants to communicate secretly with Velma. Phil encrypts his message using Velma's public key (which Velma has made available to everyone) and Phil sends the scrambled message to Velma.

2. When Velma receives the message she uses her private key to unscramble the message so that the message can be read.

3. When Velma sends a reply to Phil, she scrambles the message using Phil's public key.

4. When Phil receives Velma's reply, he uses his private key to unscramble her message.

Public key cryptography has a major advantage over secret key cryptography—there is no need to communicate secret keys up-front. Provided the private key is kept secret, confidential communication is possible using the public keys.

Combining Public Key and Secret Key Cryptography. The main disadvantage of public key cryptography is that the process of encrypting a message can cause performance problems on all but the most powerful computer systems. For this reason, public key and secret key cryptography are often combined. The following example illustrates how this works:

1. Velma wants to communicate secretly with Phil, so she obtains Phil's public key. She also generates random numbers that she will use just for this session, known as a session key.

2. Velma uses Phil's public key to scramble the session key.

3. Velma sends the scrambled message and the scrambled session key to Phil.

4. Phil uses his private key to unscramble Velma's message and extract the session key.

Once Velma and Phil have successfully exchanged the session key, they no longer need public key cryptography; communication can take place using just the session key. In other words, public key encryption is used to send the secret key then, once the secret key has been exchanged, communication takes place using secret key encryption.

This solution offers the advantages of both methods—it provides the speed of secret key encryption and the security of public key encryption.

Certificates and Certificate Authorities

The sender of a message must be sure that they have the public key belonging to the receiver. To address this, SSL uses public key certificates and Certificate Authorities.

A certificate is a digital file issued by a trusted organization known as a Certificate Authority (CA). A certificate is basically “proof of identity”. Certificates generally have a common format, usually based on ITU standards. The certificate contains information that includes the:

- Issuer—this is the organization that issues the certificates.
- Period of validity—the certificate’s start date and expiry date.
- Public key—the secret key used to encrypt data.
• Issuer’s signature—the CA digitally signs the certificate to guarantee its authenticity.

A number of companies and organizations act as Certificate Authorities, including VeriSign, Baltimore and their affiliates.

Certificate Revocation Lists

From time to time, CAs issue Certificate Revocation Lists (CRLs). CRLs contain information about certificates that can no longer be trusted; for example, because the private key has been compromised. Therefore, to trust a public key, you must also ensure that its certificate has not been revoked.
Getting Started - A Summary of the Steps

The following section summarizes the steps required to get SSL Relay up and running in a XenApp installation. A typical example is used to illustrate these steps.

**Note:** This section is intended as an overview only—it is important that you read the section "Planning Your SSL Relay Deployment" to ensure that you accurately estimate the type and number of digital certificates required for your SSL Relay deployment.

In the following example, the Citrix administrator wants to use SSL Relay to secure communications between client devices and a XenApp for UNIX server. The server is called "bagpuss"; the server is on a LAN and there are no firewalls. The server has been installed with Citrix XenApp for UNIX. The administrator has deployed SSL-enabled plugins on the client devices that access bagpuss.
To get SSL Relay up and running

1. The administrator reads the section about Planning Your SSL Relay Deployment. From her reading, she determines that a server certificate is required for bagpuss, and she decides to apply to VeriSign for this certificate.

The administrator logs on to bagpuss as the ctxssl user and runs ctxcertreq to generate a certificate request file. She labels the file “citrix”.

```
ctxcertreq citrix
```

At the prompt, she specifies the password “secret” to protect the file. Since the -filename option is not specified, the certificate request is written to “citrix.req” in the current directory.

2. The administrator sends the certificate request file to VeriSign via a Web browser.

3. VeriSign process the certificate request and issue a server certificate. The administrator is notified by email when the signed certificate is ready, and the administrator retrieves the signed certificate via a Web browser. The administrator saves the certificate file on bagpuss in: /tmp/citrix.pem.

4. The administrator logs on to bagpuss as the ctxssl user and uses ctxcertmgr to install the certificate. She includes the -response option, that indicates that the certificate is a response to a certificate request generated using ctxcertreq.

```
ctxcertmgr -response /tmp/citrix.pem
```

The system prompts for the password “secret” that is used to protect the file.

5. To configure SSL Relay to listen for connections on port 443, and to configure the forwarding list to permit redirection to ports 1494 and 80, the administrator types:

```
ctxsslcfg -add 443 -certificate citrix -forward add bagpuss:1494 -forward add bagpuss:80
```

The system prompts for the password “secret”. Since no ciphersuite is specified, the default ALL is applied (ALL includes both the commercial and government suites, ordered such that commercial is given preference).

6. To start SSL Relay on bagpuss, the administrator types:

```
ctxsrv start sslrelay
```

SSL Relay is now up and running on the server and SSL-enabled plugins can make secure connections to the server.
What to Do Next

Before you can begin using SSL Relay, you must plan how you will deploy SSL to secure communications in your XenApp installation, and obtain the appropriate digital certificates. For information, see Planning Your SSL Relay Deployment.
Planning Your SSL Relay Deployment

This section helps you to determine whether you need to deploy SSL Relay in your Citrix XenApp installation, and it considers the steps in planning an SSL Relay deployment. Topics covered in this section include:

- Determining whether SSL Relay is the appropriate solution
- Obtaining digital certificates
- Configuring ctxssl access to commands
- Planning for an attack on your security
- Planning the renewal of expired certificates

Before you can begin using SSL Relay, you must:

- Evaluate what the security risks are and determine the most appropriate solution
- Plan how you will deploy SSL in your XenApp installation
- Obtain the appropriate digital certificates
- Consider the protection of your private keys
- Install the digital certificates
- Plan how you will deal with security attacks
- Plan the renewal of expired certificates

This section guides you through each step of the planning process and discusses the issues that you need to consider before you can configure and use SSL Relay.
Choosing an Appropriate Security Solution

The first step in planning an SSL Relay deployment is to evaluate what the security risks are and then determine the most appropriate solution for your XenApp installation.

The main threats to security are:

- **Eavesdropping**—eavesdropping on sensitive information, such as user ids and passwords, is a serious threat to security as an unauthorized user could use these credentials to gain access to the XenApp installation.

- **Misrouting**—a message could, in theory, be intercepted during its transmission and re-routed to a counterfeit Web site.

- **Data manipulation**—the contents of a message might be lost, deliberately modified, or accidentally corrupted during transmission.

- **Denial of Service**—in Denial of Service attacks, access to a system or application is prevented or interrupted.

Knowing the threats, you then need to consider whether your XenApp installation is at risk of a security attack.

You may not need to be concerned about secure communications if, for example, the servers running the Web Interface, XenApp, and the Citrix XML Service are in a protected machine room and there is no reasonable way of attacking the link. Or you may decide that the additional burden of deploying a security solution outweighs the benefits.

If you consider that your XenApp installation is at risk of attack, a solution such as IPSec may be more appropriate than SSL Relay. IPSec provides secure communications between the Web server and the XenApp server, therefore, if your organization has already standardized on IPSec, SSL Relay is not required.

If you consider that your XenApp installation is at risk of attack, and your organization has not standardized on IPSec, we recommend you use SSL Relay.
Obtaining a Digital Certificate

The next step in planning your SSL Relay deployment is to determine the number and type of digital certificates that are required, and to obtain these from a suitable source.

A certificate is a digital file issued by a trusted organization known as a Certificate Authority (CA). For more information about certificates and CAs, see Certificates and Certificate Authorities.

Obtaining a digital certificate can be an involved process, therefore it is important to accurately estimate how many digital certificates you will require up-front, and to allow enough time for the process of obtaining the certificates.

This section helps you identify the number and type of certificates you will require, and the considerations you should make when deciding where to obtain certificates from.
Determining the Certificates Required

There are two main types of digital certificate:

<table>
<thead>
<tr>
<th>Identity certificate</th>
<th>This identifies a specific machine—for example, a XenApp server. The type of identity certificate that is required by SSL Relay is called a Server Certificate.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root certificate</td>
<td>This identifies the CA that signed the identity certificate. The root certificate belongs to the CA.</td>
</tr>
</tbody>
</table>

For SSL Relay to work, you require a server certificate at one end of the connection and a root certificate at the other end.

A server certificate must be installed on every XenApp server on which you plan to use SSL Relay and, in some cases, on the server running the Web Interface.

A root certificate must be installed on the client device and on the server running the Web Interface.

Certificates Required Between SSL-enabled Plugins and a Web Interface Server

In a Web Interface deployment, the security of the connection between the client device and the Web Interface is dependant on the abilities and configuration of the server running the Web Interface and the client device’s Web browser. The majority of Web browsers and Web servers support SSL, but configuration is required before the connection is secured. To do this, you require:

- A root certificate on the client device that can verify the signature of the CA on the server certificate. The root certificate is usually part of the Web browser itself, so there is no need to obtain and install a root certificate here.

- A server certificate on the server running the Web Interface—for more information about installing a server certificate, see your Web server documentation.

The following diagram shows the server and root certificates required to secure communications between SSL-enabled plugins and the server running the Web Interface:
Certificates Required Between a Web Interface Server and a XenApp Server

In a Web Interface deployment, you can use SSL to secure the connection between the Web Interface server and the XenApp for UNIX server. To do this, you require:

- A root certificate on the server running the Web Interface specifically for the Java objects. Support for VeriSign and Baltimore root certificates is already built into the Web Interface server, so there is no need to obtain and install root certificates for these CAs. However, if you choose a different CA, you will need to obtain and install the root certificates yourself.
Determining the Certificates Required

- A server certificate on the XenApp for UNIX server.

Since the Web Interface server and XenApp servers are different machines, you will require separate server certificates. You cannot use the same server certificate on both machines.

The following diagram shows the certificates required to secure communications between a Web Interface server and a XenApp server:

![Diagram showing certificates required between a Web Interface server and a XenApp server]

Typically, in a Web Interface deployment, one server runs the Citrix XML Service that provides Web Interface information. However, there may also be a backup of this server. In this case, you would deploy SSL on the main XenApp server and the backup server, therefore, you will require a separate server certificate on each of these servers.

Certificates Required Between SSL-enabled Plugins and a XenApp Server

You can use SSL to secure connections between plugins and a XenApp server. To do this you deploy SSL-enabled plugins and install SSL Relay on the server. The following certificates are required:

- A root certificate on every SSL-enabled plugin that will access the XenApp server. Support for VeriSign and Baltimore root certificates is already built into the plugins, so there is no need to obtain and install root certificates on the client device for these CAs. However, if you choose a different CA, you will need to obtain and install the root certificates yourself.

- A server certificate on the XenApp server.
The following diagram shows the certificates required to secure communications between SSL-enabled plugins and a XenApp server:

**Certificates Required for a Fully Secured Installation**

To use SSL to fully secure all communications in your XenApp installation, you must:

- Deploy an SSL-capable Web browser and SSL-capable Web server.
- Use SSL to secure communications between the Web Interface server and the XenApp server.
- Use SSL to secure communications between SSL-enabled plugins and the XenApp server.

The following diagram shows the certificates required to secure communications at all points in your XenApp and Web Interface installation.
Determining the Certificates Required
Using SSL with Load Balancing

If you are using Load Manager, ensure that you obtain and install server certificates for every load balanced server to which plugins could connect using SSL.

For example, if you have 10 load balanced XenApp servers that are capable of running your users’ applications, you will require 10 server certificates. Without the appropriate certificates, an SSL-secure connection will be unable to connect to a XenApp server.

For more information about load balancing, see the Citrix XenApp for UNIX Administrator’s Guide.
Where Do I Get Certificates From?

Once you have identified the number and type of certificates required for your SSL Relay deployment, you must decide where to obtain the certificates from.

Where you choose to obtain certificates will depend on a number of factors, including:

- Whether your organization is a Certificate Authority (CA). This is likely to be the case only in very large corporations.
- Whether your organization has already established a business relationship with a public CA.
- The fact that SSL Relay includes support for the VeriSign and Baltimore public Certificate Authorities—support for these root certificates is built into the SSL-enabled plugins and the server running the Web Interface.
- The cost of certificates, the reputation of a particular public CA, and so on.

If your organization is a Certificate Authority

If your organization is running its own Certificate Authority, you must determine whether it is appropriate to use your company’s certificates for the purpose of securing communications in your XenApp installation. Citrix recommend that you contact your Corporate Security department to discuss this, and to get further instructions on how to obtain the certificates.

If you are unsure if your organization is a Certificate Authority, contact your Corporate Security department.

If your organization is not a Certificate Authority

If your organization is not running its own Certificate Authority, you need to obtain your certificates from a public CA, such as VeriSign or Baltimore.

Obtaining a digital certificate from a public CA involves a verification process in which:

- Your organization provides corporate information so that the CA can verify that your organization is who it claims to be. This may involve other departments in your organization, such as Accounts, to provide Letters of Incorporation or similar legal documents.
- Individuals with the appropriate authority in your organization are required to sign legal agreements provided by the CA.
- The CA verifies your organization as a purchaser, therefore your Purchasing department is likely to be involved.
You provide the CA with contact details of suitable individuals who they can call if there are queries.

Therefore, obtaining a digital certificate from a public CA can be an involved process.

**Important:** If you require an additional certificate for another server, you will have to repeat the CA’s verification process. You cannot obtain a certificate for one server and use it on another. Therefore, it is important to decide at the start how many certificates you require and to allow enough time for the process of obtaining these.

**Obtaining a Root Certificate from a CA**

Support for VeriSign and Baltimore root certificates is already built into SSL-enabled plugins and the server running the Web Interface. Therefore, there is no need to obtain and install root certificates on the client device or on the Web Interface server if you are using these CAs. However, if you decide to use a different CA, you will need to obtain and install the root certificates yourself.

CAs tend to assume that you already have the appropriate root certificates (this is because most Web browsers have root certificates built-in as standard) so you will need to specifically request the root certificate. Also, there are different types of root certificate—for example; VeriSign have approximately 12 root certificates that they use for different purposes—so ensure that you obtain the correct root certificate from the CA.
Configuring ctxssl Access to Commands

Before you can use the SSL Relay command-line tools, such as ctxcertreq to generate a certificate request file, you must configure your system so that the ctxssl user can run the commands from the server console or from an ICA session. To do this, you add the /opt/CTXSssl/sbin directory (when using Solaris and HP-UX), or the /usr/lpp/CTXSssl/sbin directory (when using AIX) to the PATH variable.

To configure ctxssl access to SSL Relay commands

- If you are using a C shell, use a .login file for the ctxssl user, and add the path to the commands. For example, for HP-UX and Solaris:

```
setenv PATH ${PATH}:/opt/CTXSssl/sbin
```

For AIX:

```
setenv PATH ${PATH}:/usr/lpp/CTXSssl/sbin
```

- If you are using a Bourne, or similar, shell use a .profile file for the ctxssl user, and add the path to the commands. For example, for HP-UX and Solaris:

```
PATH=${PATH}:/opt/CTXSssl/sbin
export PATH
```

For AIX:

```
PATH=${PATH}:/usr/lpp/CTXSssl/sbin
export PATH
```
Generating or Renewing a Certificate

Once you have decided which CA to get your certificates from, the next step is to use the ctxcertreq utility to create a certificate signing request (CSR) file that you can send to the CA.

The ctxcertreq utility prompts you for the information it requires, and generates a keypair (a private key and corresponding public key). The private key is encrypted and stored locally, and the public key is used to create the CSR file.

You can also use ctxcertreq to generate a certificate renewal request file that you can send to the CA. To do this, you include the -clone option.

The following section explains how to use ctxcertreq to generate a new CSR file or a certificate renewal request file. For more information about renewing certificates, see Planning the Renewal of Expired Certificates.

What information is prompted for?

When you run ctxcertreq, you are prompted for the following information:

- The distinguished name of the subject requesting the certificate—in this case, the XenApp server.

  **Note:** When you generate a certificate renewal request, you can either accept the default details that are displayed for the distinguished name, or override these. This enables you to generate a number of requests by specifying a common name for each server, without having to re-enter all the details.

The distinguished name consists of the following information:

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN</td>
<td>Common Name. This must be set to the server’s Fully Qualified Domain Name (FQDN). The FQDN is the name that plugins use, rather than the name that local machines use. This parameter is the only one required by ctxcertreq, however, your CA may also require the following parameters to be present.</td>
</tr>
<tr>
<td>C</td>
<td>Country. This is a two letter country code; for example ‘GB’.</td>
</tr>
<tr>
<td>ST</td>
<td>State or Province.</td>
</tr>
<tr>
<td>L</td>
<td>Locality.</td>
</tr>
<tr>
<td>O</td>
<td>Organization.</td>
</tr>
<tr>
<td>OU</td>
<td>Organizational Unit (for example, a department).</td>
</tr>
</tbody>
</table>

**Caution:** You must provide the exact information for the distinguished name because it is not validated by ctxcertreq. If the information you provide is incorrect, the certificate becomes useless and a new certificate request will be required which will incur an additional payment to the CA.
Generating or Renewing a Certificate

- A database password that will be used to encrypt the private key.
- A number of random keystrokes. These keystrokes are used to generate the keypair.
To generate a CSR file

1. Log on to the server as the ctxssl user.

2. At the command prompt, type:

   `ctxcertreq identifier [ -filename filename ] [ -clone clone-identifier ]`

   The following table explains the options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Use this option to:</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>identifier</code></td>
<td>Give the certificate request a unique label to identify it. This label is used by the SSL Relay tools and is not included in the certificate request file that you send to the CA.</td>
</tr>
<tr>
<td><code>-filename</code></td>
<td>Specify the file the certificate request is written to, where <code>filename</code> is the name of the file. If you do not include this option, the certificate request is written to <code>identifier</code>.req in the current directory (where identifier is the label you specified using the identifier option).</td>
</tr>
<tr>
<td><code>-clone</code></td>
<td>Renew a certificate that is due to expire, where <code>clone-identifier</code> is the identifier of the existing server certificate. The distinguished name information in the existing certificate can be copied to the certificate request file. This option can be used to request a group of similar certificates, as well as renewing a certificate.</td>
</tr>
</tbody>
</table>

3. At the prompt, type in the distinguished name parameters. If you are generating a certificate renewal request, you can accept the default distinguished name by pressing ENTER.

4. At the prompt, type in the database password that will be used to encrypt the private key.

5. Confirm the database password.

6. At the prompt, start typing. It does not matter what keys you press; you can type letters, numbers, symbols, punctuation marks, and control characters. Keep typing until `ctxcertreq` tells you to stop.
After you create the CSR file, the next step is to send this file to the CA for verification and signing. For information about submitting a CSR, contact the CA or visit their Web site.
Preparing for an Attack on Your Security

When planning your SSL Relay deployment, you must consider how you will monitor for attacks made on your security, once SSL Relay is up and running on your system.

If your organization has a standard monitoring and audit procedure, you must determine how SSL Relay will fit into this procedure. If you are currently operating a third party Intrusion Detection System (IDS), you can use this to monitor the SSL Relay server. Note however that SSL Relay does not currently support automatic integration with any third party IDSs.

This section discusses points to consider when preparing for an attack on your security, and describes what happens in misrouting, which is the most common type of attack.

Misrouting

If a message is intercepted during its transmission and re-routed to a counterfeit Web site, this is known as misrouting. If misrouting occurs:

- Between the client device and the Web Interface server, an error is displayed on the client device. To ensure users cannot continue regardless, use the client lock down feature of your Web browser, so that the connection cannot proceed. For information about the client lock down feature, see the documentation that accompanies your Web browser.

- Between the Web Interface server and the XenApp for UNIX server, the Web Interface server logs an error message. For information about error messages, see the Web Interface documentation.

- Between the client device and the XenApp for UNIX server, the plugin displays a specific error message.
Planning the Renewal of Expired Certificates

Digital certificates expire after a period of time; usually a year. Typically, your CA will send you a reminder. Therefore, when planning your SSL Relay deployment, you should also plan for the renewal of your certificates.

If your digital certificates are issued by a public CA, you must submit a certificate renewal request to the CA, together with the appropriate billing information. If your organization is a Certificate Authority, contact your Corporate Security department for information about renewing certificates.

The process of renewing a certificate can be involved, therefore, it is important to allow enough time for this process, before your existing certificates expire.

You may also have to plan for a suitable overlap period, to allow adequate time to transfer from old certificates to new ones. For example, if an existing certificate expires on the 6th of June, you may want the new certificate to start on the 4th of June, to allow time to switch to the new certificate.

When a certificate expires, you can use a different CA, rather than renewing the existing certificate.

Renewing a Certificate

To generate a certificate renewal request file that you can send to the CA, use ctxcertreq with the -clone option. For information, see Generating or Renewing a Certificate.

For more information about renewing certificates, go to your CA’s website.

For information about displaying certificate expiration dates, see To display server certificate information.

Note: Root certificates also expire after a period of time, however, they are typically valid for up to 10 years.
What to Do Next

After you have planned your SSL Relay deployment and obtained the appropriate digital certificates, the next step is to install the certificates. See Installing Digital Certificates for more information.
Installing Digital Certificates

This section describes how to install server certificates on a XenApp for UNIX server.

The issuing of certificates is an online process. Once you have received a signed certificate from the CA, the next step is to install the certificate on the appropriate machine.

The following section describes how to install a server certificate on a XenApp server. It also tells you where to find information about installing root and server certificates on a server running the Web Interface or on SSL-enabled plugins. The section also discusses the importance of protecting the private keys.
Protecting the Private Key

Because SSL is based upon public key cryptography (also known as asymmetric key cryptography) there are always two keys:

- A public key that is made available to everyone.
- A private key that is kept secret.

The server certificate contains both the public and private keys; each of these keys must be installed on the server running SSL Relay.

You must protect the private key at all times. If you do not protect this key, not only is your security compromised but you have no legal redress in the event of a security attack.

If your organization already has a strategy for protecting and managing private keys, contact your Corporate Security department to discuss the correct procedures. If your organization currently has no methods for managing and protecting keys, you will need to formulate a strategy before installing your certificates.

To ensure private keys are kept secret, SSL Relay protects your keys using UNIX operating system security. Keys are stored in a directory that requires special permissions and that only the ctxssl user can access.

**Caution:** Although SSL Relay attempts to protect your private keys to the maximum possible extent, if an unauthorized user can access the XenApp server that holds the private key and log on as root, they can get hold of the private key. This also has implications for backups—if you back up the XenApp server, the private key is also backed up. Therefore, you must consider how you will protect your backups; for example, by keeping them in a secure store.
Installing a Server Certificate on a Server

Certificates are installed using the ctxcertmgr command. You install a certificate from the certificate file that you receive from the CA. Server certificates are installed in the /var/CTXSssl directory of the XenApp server.

How you install a certificate depends upon whether you used ctxcertreq to generate the certificate request or not.

**Note:** Before you can use the SSL Relay command-line tools, you must configure your system so that the ctxssl user can run the commands. Configure this now, if you have not already done so; for information, see Configuring ctxssl Access to Commands.
To install a server certificate requested using ctxcertreq

If you use ctxcertreq to generate a certificate request, ctxcertreq generates a private key and prompts you for a password to protect the file. When you receive the signed certificate from the CA, you need to install the certificate on the XenApp server and match it to the private key and password.

To do this, you use ctxcertmgr to install the certificate and include the -response option. The -response option indicates that the certificate is a response to a certificate request generated using ctxcertreq. A new certificate is created which is stored on the XenApp server.

1. Log on to the server as the ctxssl user.

2. At the command prompt, type:

   ctxcertmgr -response filename [ -dbpassword db-password ]

   where filename specifies the certificate file supplied by the CA.

The following table describes the options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Use this option:</th>
</tr>
</thead>
<tbody>
<tr>
<td>-response</td>
<td>To indicate the certificate is a response to a certificate request generated using ctxcertreq.</td>
</tr>
<tr>
<td>-dbpassword</td>
<td>To specify the password used to protect the certificate on the XenApp server. This is the database password you supplied when you ran ctxcertreq. If you include the -dbpassword option, you must use the db-password parameter to specify the new password, which should be no larger than 255 characters. Note that this option is only used if you are including commands in a shell script; otherwise you are prompted for the password. Using -dbpassword will display the password on the terminal, and enter it into the user’s command line history.</td>
</tr>
</tbody>
</table>

Example

Using ctxcertreq, a new certificate request file is generated with the identifier “citrix”. A private key is also generated and the password “secret” specified to protect the file. The new certificate is received from the CA—this file is called “cert.pem” and it is saved in the /ssl directory on the XenApp server.

To add the certificate to the server and match it to the private key and password, type:

ctxcertmgr -response /ssl/cert.pem
To install a server certificate requested using ctxcertreq

You are prompted for the db-password “secret”.
To install a server certificate not requested using ctxcertreq

If you generated the certificate request using a tool other than ctxcertreq, use ctxcertmgr with the -import option to install the certificate.

1. Log on to the server as the ctxssl user.

2. At the command prompt, type:

   ctxcertmgr -import identifier -filename filename [-format format] [-keyfilename key-filename] [-dbpassword db-password] [-filepassword file-password]

The following table describes the options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Use this option:</th>
</tr>
</thead>
<tbody>
<tr>
<td>-import</td>
<td>To add a certificate to the XenApp server. Use the identifier parameter to give your certificate a unique label. This label is used to easily identify the certificate in future.</td>
</tr>
<tr>
<td>-filename</td>
<td>To specify the certificate file supplied by the CA, where filename is the location of the file. If the CA supplies the certificate as two separate files (one file containing the private key; the other containing plaintext information about the certificate) use the -filename option to specify the location of the file containing plaintext information.</td>
</tr>
<tr>
<td>-format</td>
<td>To specify the format of the certificate file supplied by the CA. You can import PEM, NET, DER, PKCS12, and MKS file formats. If you do not specify a format, the system attempts to auto-detect the format; if it cannot detect the format, an error message is displayed.</td>
</tr>
<tr>
<td>-keyfilename</td>
<td>If the CA supplies the certificate as two separate files (one file containing the private key; the other containing plaintext information about the certificate). Use the key-filename parameter to specify the location of the file containing the private key. Note that, in this case, you would use the -filename option to specify the location of the file containing plaintext information.</td>
</tr>
<tr>
<td>-dbpassword</td>
<td>To specify the new password that you will use to protect the certificate on the XenApp server. If you include the -dbpassword option, you must use the db-password parameter to specify the new password. This should be no larger than 255 characters.</td>
</tr>
<tr>
<td>-filepassword</td>
<td>To specify the password that the CA used to protect the certificate file. When a CA sends you a certificate, the certificate is protected using a password. You need this password to extract the certificate from the file. The CA may supply this password in a separate email. If you include the -filepassword option, you must use the file-password parameter to specify the CA’s password.</td>
</tr>
</tbody>
</table>
Example - the CA emails the server certificate as one file

The CA sends you a signed certificate file in PEM format. You save this file in the /certs directory on your server, and call it “file1.pem”. The private key is protected with the password “secret”.

To install the server certificate on your server, using the new password “confidential” and the identifier “my_certificate”, type the command:

```
ctxcertmgr -import my_certificate -filename /certs/ctxssl/file1.pem
```

You are prompted for the db-password “confidential” and the file-password “secret”.
Example - the CA emails the server certificate as two files

The CA sends you the server certificate as two separate files. One file contains plaintext information about the certificate; the other contains the private key which the CA protects with the password “secret”. The files are in PEM format. You call the plaintext file “file1.pem” and store it in the /ssl directory. You call the private key file “file2.pem” and save it to the home directory /home/ctxssl that only you can read.

To install the server certificate on your server, using the new password “confidential” and the identifier “my_certificate”, type the command:

```
ctxcertmgr -import my_certificate -filename /ssl/file1.pem -keyfilename /home/ctxssl/file2.pem -dbpassword confidential -filepassword secret
```

Only use -dbpassword and -filepassword if you are including commands in a shell script.

**Note:** For information about installing server certificates on a server running the Web Interface, see the [Web Interface documentation](#).
Installing a Root Certificate

A root certificate must be installed on every SSL-enabled plugin or on the server running the Web Interface, depending upon how you plan to use SSL Relay in your XenApp installation.

Installing Root Certificates on SSL-enabled Plugins

A root certificate is required on every SSL-enabled plugin that will access the XenApp server. This means that when you roll out plugins to your users, you will need to bundle the root certificate along with the plugin files.

Support for VeriSign and Baltimore root certificates is already built into SSL-enabled plugins, so there is no need to install root certificates on the client device for these CAs. However, if you choose a different CA, you will need to install the root certificates yourself.

Note: If the client device is using the Windows Operating System, the root certificates are automatically available for many public CAs. However, the root certificates are not, by default, available for your own organization’s CA. It is the responsibility of your Corporate Security Department to install these in Windows. For more information about administering these root certificates, see the online plug-in or Plug-in for Hosted Apps documentation.

Installing Root Certificates on a Web Interface Server

By default, the Citrix Web Interface Extension (on the server running the Web Interface) contains root certificates for VeriSign and Baltimore. Therefore, if you have chosen to use VeriSign or Baltimore as your CA, you do not have to install root certificates on the server running the Web Interface.

However, if you have chosen to use a CA other than VeriSign or Baltimore, you must add the CA’s root certificate to the Citrix Web Interface Extension—see the Web Interface documentation for information about how to do this.
What to Do Next

After you have installed the appropriate digital certificates, the next step is to configure SSL Relay and get it up and running. See To configure SSL Relay ready for use for more information.
Configuring SSL Relay

This section describes how to enable and configure SSL Relay ready for use. Also explained is how to maintain SSL Relay and the digital certificates stored on the XenApp server.
To enable or disable SSL Relay

You can enable or disable SSL Relay at any time after installation by modifying the SSL_ENABLED parameter in /var/CTXSmf/ssl/config.

**Note:** You must stop and restart SSL Relay using the ctxsrv stop sslrelay and ctxsrv start sslrelay commands for these changes to take effect.

1. Do one of the following:
   
   - To enable SSL Relay, write SSL_ENABLED=1 to /var/CTXSmf/ssl/config.
   - To disable SSL Relay, write SSL_ENABLED=0 to /var/CTXSmf/ssl/config.
Configuring SSL Relay Ready for Use

After you have obtained and installed your digital certificates, the next step is to configure the SSL Relay ready for use. The following section describes in detail what you must configure on the XenApp server, and explains how to use the ctxsslcfg command to do this.

What Do I Need to Configure?

Before you can use SSL Relay for the first time, you must:

- Specify the TCP port that SSL Relay will listen for connections on.
- Configure the ciphersuite (encryption type) that SSL Relay will accept.
- Configure the forwarding list (the port numbers and addresses that plugins can connect to).

You must also specify the server certificate you installed previously on the XenApp server, together with the password you used to protect the private key.

Specifying the TCP Port that SSL Relay Listens On

You must specify the port that SSL Relay will listen for connections on. By default, SSL Relay listens on TCP port 443, which is the standard port for SSL-secured communications.

You can configure SSL Relay to listen on a different port; for example, you may have to do this if there is already a secure Web server (such as IIS) running on the server that uses port 443. However, ensure that the port you choose is open on any firewalls between the Web server and the server running SSL Relay.

Note: Use TCP port 443 for SSL-secured communications, whenever possible. If you configure SSL Relay to listen on a port other than 443, you must also configure the other parts of your installation accordingly. Therefore, if you are using the Web Interface, you must configure the Web server to use a port other than 443. For SSL-enabled plugins, you must configure each plugin, on a per-application basis, to use the different port number.

Configuring the Ciphersuite

The process of establishing a secure connection involves negotiating the ciphersuite that will be used during communications. A ciphersuite defines the encryption type that will be used; it defines the cipher algorithm and its parameters, such as the size of the keys.

Negotiation of the ciphersuite involves the plugin telling SSL Relay the ciphersuites it is capable of handling, and SSL Relay telling the plugin the ciphersuite that will be used during communication. Therefore, you must configure SSL Relay to use the appropriate ciphersuite for your communications.
SSL Relay supports two main categories of ciphersuite: COM (commercial) and GOV (government). The ALL option includes both the commercial and government suites, ordered such that commercial is given preference.

- **COM (commercial)**—the commercial ciphersuites are:
  - `SSL_RSA_WITH_RC4_128_MD5` or `{0x00,0x04}
  - `SSL_RSA_WITH_RC4_128_SHA` or `{0x00,0x05}

- **GOV (government)**. Some organizations, including US government organizations, require the use of government-approved cryptography to protect “sensitive but unclassified data”. The government ciphersuite is:
  - `SSL_RSA_WITH_3DES_EDE_CBC_SHA` or `{0x00,0x0A}

### Configuring the Forwarding List

When SSL Relay receives an SSL-secured connection, it decrypts the data and redirects the connection, usually to the XenApp processes or to the Citrix XML Service.

By default, XenApp listens for ICA connections on port number 1494, and the XML Service communicates with the Web Interface server on port number 80. Therefore, you must configure SSL Relay to permit redirection to these ports (or to different port numbers you assigned to ICA and the XML Service), as shown in the following diagram:

![Diagram of SSL Relay configuration](image)

You can also configure SSL Relay to control which addresses plugins can connect to. For example, you may want to restrict access to a particular set of addresses.

The ports and addresses you permit access to are known as the **forwarding list** for the TCP port.
Caution: Citrix recommend that you configure SSL Relay to restrict access to specific ports only. If, instead, you configure SSL Relay to allow access to ports other than those used by ICA and the XML Service, you may allow users to connect to SSL Relay and gain access to unauthorized ports on the server.
To configure SSL Relay ready for use

You use the ctxsslcfg command to configure SSL Relay.

1. Log on to the server as the ctxssl user.

2. At the command prompt, type:

```bash
ctxsslcfg -add port [ -certificate identifier ] [ -dbpassword db-password ] [ -ciphersuite { GOV | COM | ALL } ] [ -forward { add | remove } { * | { hostname | IP-address | * }:{ port | * } } ]
```

The following table explains the options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Use this option to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>-add</td>
<td>Add the port number that SSL Relay will listen for connections on. Specify the port number using the <code>port</code> parameter. For example: <code>-add 443</code> specifies port number 443.</td>
</tr>
<tr>
<td>-certificate</td>
<td>Specify the server certificate to be used during secure communications. This certificate must be installed on the server. Use the <code>identifier</code> parameter to specify the certificate using the label you gave the certificate. For example if you installed a certificate labelled “citrix”, type: <code>-certificate citrix</code>.</td>
</tr>
<tr>
<td>-dbpassword</td>
<td>Specify the password with which the certificate’s private key is decrypted.</td>
</tr>
<tr>
<td></td>
<td>This password must match the password you specified using the <code>db-password</code> parameter when you installed the certificate. For example, if you specified a password of “confidential” when you installed the certificate, type: <code>-dbpassword confidential</code>.</td>
</tr>
<tr>
<td></td>
<td>If you do not include the <code>-dbpassword</code> option in the command, you are prompted for a password.</td>
</tr>
<tr>
<td>-ciphersuite</td>
<td>Specify the ciphersuite that will be used during secure communications—COM, GOV or ALL. If you do not specify a ciphersuite, ALL is used by default.</td>
</tr>
</tbody>
</table>
To configure SSL Relay ready for use

| -forward          | Configure the forwarding list for this port number. The forwarding list defines the port numbers (typically 1494 and 80) and addresses that SSL Relay permits access to. Use the add parameter to specify that you are adding an entry to the forwarding list. For example, on the server “mandix” to allow access on ports 1494 and 80, type: -forward add mandix:1494 -forward add mandix:80

You can use an * (asterisk) as a wildcard to mean all port numbers or all addresses. However, because the asterisk represents “zero or more characters” in UNIX, remember to include quotation marks. For example, to allow access to all addresses on port 1494, type: -forward add “*:1494”

A single * (asterisk) is equivalent to specifying *:*.. For example, to allow access to all addresses and all ports, type: -forward add “*”

Do not use the term “localhost” as the hostname. |

After you have configured SSL Relay ready for use, you are ready to start SSL Relay on the XenApp server; see To start the SSL Relay for more information.

**Example**

On the server “radish”, you want to configure the SSL Relay to listen for connections on port 443, using the identity certificate labelled “citrix”, and to allow access to ports 1494 and 80. Type:

ctxsslcfg -add 443 -certificate citrix -forward add radish:1494 -forward add radish:80

Because no password is specified, you are prompted for one. And, since no ciphersuite is specified, the default of ALL is used (the ALL suite includes both commercial and government suites, ordered such that commercial is given preference).
To start the SSL Relay

To start SSL Relay on a XenApp for UNIX server, use the ctxsrv start command.

1. Log on to the server as the ctxssl user.

2. At the command prompt, type:

   ctxsrv start sslrelay

SSL Relay runs as a daemon on the XenApp for UNIX server. In future, when XenApp is started on the server, the SSL Relay daemon also starts automatically.
To stop the SSL Relay

Use the ctxsrv stop command to stop SSL Relay on a XenApp for UNIX server.

1. Log on to the server as the ctxssl user.
2. At the command prompt, type:

   ctxsrv stop sslrelay

If all the XenApp processes are stopped on the server using ctxsrv stop all, the SSL Relay daemon also stops.
Displaying a TCP Port’s Configuration

Using the ctxsslcfg -list command, you can display summary information about all the TCP ports configured for incoming SSL Relay connections on a XenApp server, or information about a particular TCP port’s configuration.
To display summary information for all the ports

1. Log on to the server as the **ctxssl** user.

2. At the command prompt, type:

   `ctxsslcfg -list`

   ![Console Output]

   Port  CipherSuite Certificate
   443   COM       goliath
   444   COM       goliath
To display a particular port’s configuration

1. Log on to the server as the ctxssl user.
2. At the command prompt, type:
   
   ctxsslcfg -list port

   where port is the port number you want to display details for.
Changing the SSL Relay Configuration

You can change the configuration of SSL Relay on a server using the ctxsslcfg command. You can add, edit, move, copy, and remove a TCP port's configuration, or change a port's forwarding list. You can also update the server certificate or change the ciphersuite.

**Important:** You must stop and restart SSL Relay using the ctxsrv stop sslrelay and ctxsrv start sslrelay command for these changes to take effect.
To add a new TCP port

You can add a new TCP port to the list of ports on which SSL Relay listens for incoming connections.

1. Log on to the server as the ctxssl user.

2. At the command prompt, type:

   `ctxsslcfg -add port [ -certificate identifier ] [ -dbpassword db-password ] [ -ciphersuite { GOV | COM | ALL } ] [ -forward { add | remove } { * | { hostname | IP-address | * }:{ port | * } } ]`

3. Stop and restart SSL Relay.

For more information about the options and parameters, see To configure SSL Relay ready for use.
To edit a port’s configuration

You can edit a particular TCP port’s configuration, or the configuration of every TCP port that listens for SSL connections, using the ctxsslcfg -edit command.

1. Log on to the server as the ctxssl user.

2. Do one of the following:

   - To edit a particular port’s configuration, at the command prompt type:

     ```
     ctxsslcfg -edit port [-certificate identifier] [-dbpassword db-password] [-ciphersuite { GOV | COM | ALL }] [-forward { add | remove }] { * | { hostname | IP-address } | { port | * } } [-force]
     ```

     where:

     - **port** is the port number of the TCP port you want to edit.

     - **-force** disconnects any existing connections that are illegal as a result of your changes.

   - To edit the configuration of all ports, at the command prompt type:

     ```
     ctxsslcfg -edit all [-certificate identifier] [-dbpassword db-password] [-ciphersuite { GOV | COM | ALL }] [-forward { add | remove }] { * | { hostname | IP-address } | { port | * } } [-force]
     ```

     For more information about the options and parameters, see To configure SSL Relay ready for use.

3. Stop and restart SSL Relay.
To move a port’s configuration

You can move an existing port’s configuration to another port on the XenApp server.

For example, if you decide to install a secure Web server on port 443, you must move the SSL Relay port to another port.

1. Log on to the server as the ctxssl user.

2. At the command prompt, type:
   
   `ctxsslcfg -move old_port new_port`
   
   where:

   *old_port* is the port number containing the configuration you want to move.

   *new_port* is the new port number you want to move the configuration to.

3. Stop and restart SSL Relay.

Example

To move the configuration for TCP port 443 to port 444, type:

`ctxsslcfg -move 443 444`
To copy a port’s configuration

You can copy an existing port’s configuration to another port on the server.

1. Log on to the server as the ctxssl user.
2. At the command prompt, type:

   `ctxsslcfg -copy old_port new_port`

   where:

   * `old_port` is the port number containing the configuration you want to copy.
   * `new_port` is the new port number you want to copy the configuration to.

3. Stop and restart SSL Relay.

Example

To copy the configuration for TCP port 444 to port 443, type:

`ctxsslcfg -copy 444 443`
To remove a port’s configuration

You can delete a port's configuration on the server.

1. Log on to the server as the ctxssl user.

2. At the command prompt, type:

   ctxsslcfg -remove port

   where:

   port is the port number you want to delete.

3. Stop and restart SSL Relay.

Example

To remove TCP port 443’s configuration, type:

ctxsslcfg -remove 443
Managing Your Server Certificates

This section describes how to display information about the server certificates installed on a XenApp server, how to export a server certificate to another server, and how to remove a certificate.
To display server certificate information

You can display information about the server certificates stored on a XenApp server using the ctxcertmgr command. Only non-encrypted information is displayed, such as the certificate’s expiry date. The private key is never displayed.

1. Log on to the server as the ctxssl user.

2. At the command prompt, type:

   ctxcertmgr -list

   ![ctxcertmgr screenshot]

   About Start and Expiry Dates

   Each server certificate issued by a CA includes a *period of validity* field. The period of validity includes a:

   - *not before* time. This is the certificate’s start date—until this period is reached, the certificate is considered invalid.

   - *not after* time. This is the certificate’s expiry date—after this period, the certificate is considered invalid.
To export a certificate to another server

You can export a copy of a server certificate to another XenApp server using the ctxcertmgr command.

For example, you want to replace an existing server running SSL Relay with a new machine. You install XenApp on the new machine. However, to enable SSL Relay on the new machine, you must export the server certificate from the old machine onto the new machine. To do this, you use the ctxcertmgr command to export the certificate to a file. Then, you use the ctxcertmgr command to import the certificate from this file to the new server.

Passwords are used to protect the certificate at each stage of the transfer.

1. Log on as the ctxssl user to the server where the certificate is currently installed.

2. To export a certificate to a file, at the command prompt, type:

   ctxcertmgr -export identifier -filename filename [-format { PEM | DER } [ -keyfilename key-filename ] [ -dbpassword db-password ] [ -filepassword file-password ]

   The following table describes the options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Use this option:</th>
</tr>
</thead>
<tbody>
<tr>
<td>-export</td>
<td>To export a certificate. The identifier parameter is the label you assigned the certificate when you installed it.</td>
</tr>
<tr>
<td>-filename</td>
<td>To specify the name of the file that you want to export the certificate to.</td>
</tr>
<tr>
<td></td>
<td>To export the certificate as two separate files (one file containing the private key; the other containing plaintext information about the certificate) use the -filename option to specify the name of the file containing plaintext information.</td>
</tr>
<tr>
<td>-format</td>
<td>To specify the format of the export file. For export, files must be in PEM or DER format. If you do not specify a format, the certificate is exported in PEM format.</td>
</tr>
</tbody>
</table>
To export a certificate to another server

- **-keyfilename**
  To export the certificate as two separate files (one file containing the private key; the other containing plaintext information). Use the *key-filename* parameter to specify the name of the file containing the private key. Note that, in this case, you would use the *-filename* option to specify the name of the file containing plaintext information.

  If you export the certificate in PEM format, you can export to a single file or to two separate files, therefore *-keyfilename* is optional. If you export the certificate in DER format, you must export to two separate files, therefore *-keyfilename* is a required option.

- **-dbpassword**
  To specify the password that currently protects the certificate. If you include the *-dbpassword* option, use the *db-password* parameter to specify the password. If you do not include the *-dbpassword* option, you are prompted for a password.

- **-filepassword**
  To specify a new password to protect the file. If you include the *-filepassword* option, use the *file-password* parameter to specify the password. If you do not include the *-filepassword* option, you are prompted for a password.

3. To import a certificate to a new server (from the file that you exported the certificate to) at the command prompt, type:

```plaintext
ctxcertmgr -import identifier -filename filename [-format format ] [ -keyfilename key-filename ]
```

where:

*filename* is the file that you exported the certificate to.

You are prompted for:

*file-password* which is the password that protects the file.

*db-password* which is the new password that will protect the certificate.

For more information about importing certificates, and for a full description of the options, see Installing a Server Certificate on a Server.

**Example**

You want to export a server certificate that has the identifier “Citrix” to another XenApp server. You export the certificate to a file called “citrix_systems.pem”. The certificate is currently protected on the server using the password “cabbage”. You use the new password “broccoli” to protect the file.

To export the certificate, type:

```plaintext
ctxcertmgr -export Citrix -format pem -filename citrix_systems.pem
```

You are prompted for the db-password “cabbage” and file-password “broccoli”. 


Next, you import the certificate from the “citrix_systems.pem” file to the new server. You use the new password “carrot” to protect the file. Type:

ctxcertmgr -import Citrix -format pem -filename citrix_systems.pem

You are prompted for the file-password “broccoli” and db-password “carrot”.

The following diagram shows the use of the db-password and file-password:

```
Old Server
  Server Certificate
  db-password = cabbage

      export

      File
      file-password = broccoli

      import

New Server
  Server Certificate
  db-password = carrot
```
To remove a stored certificate

You can delete a certificate from a XenApp server using the ctxcertmgr command.

1. Log on to the server as the ctxssl user.

2. At the command prompt, type:

   `ctxcertmgr -remove identifier`

   where `identifier` is the label you assigned the certificate when you installed it.

**Example**

To remove a server certificate that has the identifier “Citrix”, type:

`ctxcertmgr -remove Citrix`
SSL Relay Command Reference

This section describes the Citrix XenApp SSL Relay for UNIX command-line utilities. The commands listed in this section are:

ctxcertmgr Install and manage server certificates

ctxcertreq Generate a new certificate request file or a certificate renewal request file

ctxsslcfg Configure SSL Relay

**Note:** For information about the ctxsrv command, see the *Citrix XenApp for UNIX Administrator’s Guide*. 
ctxcertmgr

Description

ctxcertmgr manages server certificates.

Using ctxcertmgr you can add server certificates on a XenApp server. You can also display information about certificates, export a certificate to another server, and remove a certificate.

Syntax

| ctxcertmgr                        | [ -server | -root ] [ -import identifier | -export identifier ]
|                                  | -filename filename [ -format format ] [ -keyfilename key-filename ] [ -dbpassword db-password ] [ -filepassword file-password ]
| ctxcertmgr                        | [ -server ] -response filename [ -dbpassword db-password ]
| ctxcertmgr                        | [ -server | -root ] -list
| ctxcertmgr                        | [ -server | -root ] -remove identifier

Options

-server Specifies that the certificate is a server certificate. This is the default.
-root Specifies that the certificate is a root certificate. SSL Relay does not require root certificates to be installed on the server. However, if you want to use ctxcertmgr to maintain a store of root certificates, use the -root option.
-import Adds a certificate and its private key to the server.
-export Exports a certificate and its private key to a file.
.filename If you are adding a certificate to the server using the -response option, use the -filename option to specify the signed certificate file supplied by the CA.

If you are adding a certificate to the server using the -import option, use the -filename option to specify the certificate file supplied by the CA, and use the -keyfilename option to specify the file containing the private key.

If you are exporting a copy of a certificate to another server using the -export option, use the -filename option to specify the file that you want to export the certificate to.
**ctxcertmgr**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-format</td>
<td>Specify the format of the certificate file. If you are adding a certificate to the server using the -import option, and you do not specify a format, the system attempts to auto-detect the format; if it cannot detect the format, an error message is displayed. If you are exporting a certificate to file using the -export option, the format must be PEM or DER. Note that every format, except PEM and DER, requires the private key and the server certificate to be in the one file. With PEM format, the private key and server certificate can be in one file or in separate files. With DER format, the private key and server certificate must be in separate files.</td>
</tr>
<tr>
<td>-keyfilename</td>
<td>If you are adding a certificate to the server using the -import option, and the CA supplies the certificate as two separate files (one file containing the private key; the other containing plaintext information about the certificate) use the -keyfilename option to specify the file containing the private key. Note that, in this case, you would use the -filename option to specify the file containing the certificate information. If you are exporting a certificate to file using the -export option, use the -keyfilename option to export the certificate as two separate files (one file containing the private key; the other containing certificate information). Use the key-filename parameter to specify the name of the file containing the private key. Note that, in this case, you would use the -filename option to specify the name of the file containing plaintext information.</td>
</tr>
<tr>
<td>-dbpassword</td>
<td>Use this option if you are including the ctxcertmgr command in a shell script; otherwise you are prompted for the password. If you are adding a certificate to the server using the -import option, use this option to specify the new password that you will use to protect the certificate. If you are exporting a certificate to file using the -export option, use this option to specify the password you used to protect the certificate. If you are installing a certificate using the -response option, use this option to specify the database password you supplied when you ran ctxcertreq. If you include the -dbpassword option, you must use the db-password parameter to specify the password.</td>
</tr>
</tbody>
</table>
If you are adding a certificate to the server using the `-import` option, use this option to specify the password that the CA used to protect the file. The certificate management software may have supplied this password in a separate email.

If you are exporting a certificate to file using the `-export` option, use this option to specify a new password to protect the file.

If you include the `-filepassword` option, you must use the `file-password` parameter to specify the password.

Indicates the certificate is a response to a certificate request generated using ctxcertreq.

Displays information about the server certificates stored on the server. Only non-confidential information is displayed, such as the certificate’s expiry date. The private key is never displayed.

Removes a certificate from the server.

A unique label you give your certificate. This label can be used to easily identify the certificate in future.

The name of the file you are importing from or exporting to.

The format of the certificate file—PEM, NET, DER, PKCS12, and MKS formats are supported if you are importing a certificate; PEM and DER formats are supported if you are exporting a certificate.

The file containing the private key.

The new password used to protect the certificate while it is installed on the server.

The password you used to protect the file, or a new password you want to use to protect the file, depending upon whether you are importing or exporting a certificate.

**Remarks**

You must be the ctxssl user to run this command.
**ctxcertreq**

**Description**

ctxcertreq generates a certificate request file.

Using ctxcertreq you can create a Certificate Signing Request (CSR) file that you can send to a CA. You can create a CSR file for a new certificate, or for a certificate that you want to renew.

ctxcertreq prompts you for the distinguished name of the subject requesting the certificate (in this case, the XenApp server), and a database password that will be used to protect the private key.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>ctxcertreq identifier [ -filename filename ] [ -clone clone-identifier ]</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Options</strong></td>
<td></td>
</tr>
<tr>
<td>-filename</td>
<td>The file the CSR is written to. If you do not include this option, the CSR is written to identifier.req in the current directory, where identifier is the unique label you give the certificate.</td>
</tr>
<tr>
<td>-clone</td>
<td>Use this option to generate a CSR based upon an existing certificate. The existing certificate is used as a template for the CSR. This is useful when you want to create a number of similar CSRs, or renew an existing certificate. At the prompts, the distinguished name information defaults to the information contained in the existing certificate. Press Enter to accept the defaults, or change the information as required. Remember to change the Common Name for each server.</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>identifier</td>
<td>A unique label you give the certificate to easily identify it in future. This label is used by the SSL Relay tools and is not included in the CSR file that you send to the CA.</td>
</tr>
<tr>
<td>filename</td>
<td>The name of the file you are writing the CSR to.</td>
</tr>
<tr>
<td>clone-identifier</td>
<td>The identifier of the existing server certificate.</td>
</tr>
</tbody>
</table>

**Remarks**

You must be the ctxssl user to run this command.
ctxsslcfg

Description

ctxsslcfg configures SSL Relay.

Using ctxsslcfg you can specify a TCP port that SSL Relay listens for connections on, configure the ciphersuite that SSL Relay will use, and specify the TCP port’s forwarding list.

You cannot make changes to SSL Relay dynamically. You must stop and restart SSL Relay for any changes to take effect. You must be the ctxssl user to run this command.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxsslcfg -add</td>
<td>Adds a port that SSL Relay will listen for connections on.</td>
</tr>
<tr>
<td>-certificate</td>
<td>Specifies the server certificate to be used during secure communications.</td>
</tr>
<tr>
<td>-dbpassword</td>
<td>Specifies the password with which the certificate’s private key is decrypted.</td>
</tr>
<tr>
<td>-ciphersuite</td>
<td>Specifies the ciphersuite that will be used during secure communications.</td>
</tr>
<tr>
<td>-forward</td>
<td>Specifies a TCP port’s forwarding list.</td>
</tr>
<tr>
<td>-edit</td>
<td>Edits a particular TCP port’s SSL Relay configuration.</td>
</tr>
<tr>
<td>-move</td>
<td>Moves an existing port’s configuration to another port on the server.</td>
</tr>
<tr>
<td>-remove</td>
<td>Removes a port from SSL Relay’s forwarding list.</td>
</tr>
<tr>
<td>-list</td>
<td>Lists all configured ports for SSL Relay.</td>
</tr>
</tbody>
</table>

Options

- **-add** Adds a port that SSL Relay will listen for connections on.
- **-certificate** Specifies the server certificate to be used during secure communications. This certificate must be installed on the XenApp server using the ctxcertmgr command.
- **-dbpassword** Specifies the password with which the certificate’s private key is decrypted. 
  - **-dbpassword** is optional; if you do not include it, you are prompted for a password.
- **-ciphersuite** Specifies the ciphersuite that will be used during secure communications—COM, GOV, or ALL. If you do not specify a ciphersuite, ALL is used by default.
- **-forward** Specifies a TCP port’s forwarding list. The forwarding list defines the port numbers and addresses that SSL Relay permits access to.
- **-edit** Edits a particular TCP port’s SSL Relay configuration, or the SSL Relay configuration of every TCP port that listens for SSL connections.
- **-move** Moves an existing port’s configuration to another port on the server.
-copy Copies an existing port’s configuration to another port on the server.

-remove Removes a port’s configuration from the server.

-list Displays summary information about all the TCP ports configured for incoming SSL Relay connections on a server. Specify a TCP port number to display information about a particular TCP port’s configuration.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>port</strong></td>
<td>TCP port number.</td>
</tr>
<tr>
<td><strong>identifier</strong></td>
<td>Specifies the certificate using the unique label you gave the certificate when it was added using the ctxcertmgr command.</td>
</tr>
<tr>
<td><strong>db-password</strong></td>
<td>The password that decrypts the certificate’s private key. This is the password you specified when you installed the certificate.</td>
</tr>
<tr>
<td><strong>GOV</strong></td>
<td>The government ciphersuite: SSL_RSA_WITH_3DES_EDE_CBC_SHA or {0x00,0x0A}</td>
</tr>
<tr>
<td><strong>COM</strong></td>
<td>The commercial ciphersuites: SSL_RSA_WITH_RC4_128_MD5 or {0x00,0x04} - SSL_RSA_WITH_RC4_128_SHA or {0x00,0x05}</td>
</tr>
<tr>
<td><strong>ALL</strong></td>
<td>Both the commercial and government suites, ordered such that commercial is given preference.</td>
</tr>
<tr>
<td><strong>add</strong></td>
<td>Specifies that you are adding an entry to the forwarding list.</td>
</tr>
<tr>
<td><strong>remove</strong></td>
<td>Specifies that you are removing an entry from the forwarding list.</td>
</tr>
<tr>
<td><strong>hostname</strong></td>
<td>The hostname of the server that you are permitting access to; in other words, the server SSL Relay is running on.</td>
</tr>
<tr>
<td><strong>IP-address</strong></td>
<td>The IP address of the server that you are permitting access to.</td>
</tr>
<tr>
<td><strong>all</strong></td>
<td>All ports configured for incoming SSL Relay connections.</td>
</tr>
<tr>
<td><strong>old-port</strong></td>
<td>TCP port number of an existing port that you want to copy or move.</td>
</tr>
<tr>
<td><strong>new-port</strong></td>
<td>The new TCP port number that you want to create using an existing port’s configuration.</td>
</tr>
</tbody>
</table>

**Remarks**

You must stop and restart SSL Relay for any changes to take effect.

You must be the ctxssl user to run this command.
asymmetric cryptography
    See public key cryptography.

authentication
    A security service that verifies the identity of a communicating party.

Baltimore
    An organization which operates a public Certification Authority. Support for Baltimore root certificates is already built into SSL-enabled plugins and the server running the Web Interface.

CA
    See certificate authority.

certificate
    A digital file issued by a certificate authority. A certificate acts as a “proof of identity”.

certificate authority
    A trusted organization that issues certificates.

certificate hierarchy
    In a certificate hierarchy, a CA designates one or more subordinates who in turn can designate further subordinates. The lowest subordinates in the hierarchy certify the end users.

certificate revocation list
    A list distributed by a CA of certificates that can no longer be trusted.

certificate signing request
    A file that is sent to a CA for verification and signing. You can create a CSR file for a new certificate, or for a certificate that you want to renew.

cipher
    A secret code used to scramble a message so that the message cannot be understood by parties other than the sender and the receiver.

cipher algorithm
    A set of cryptographic options.
ciphersuite

A cipher algorithm and the parameters to be used, such as the size of the keys.

Citrix SecureICA Services

The Citrix management product that provides end-to-end encryption of business-critical data and applications.

confidentiality

A security service that protects data from being read or copied by an unauthorized user.

CRL

See certificate revocation list.

cryptography

The practise of encoding messages to ensure confidentiality.

CSR

See certificate signing request.

ctxcertreq

A command line tool for generating a certificate request file that can be sent to a CA. You can use ctxcertreq to create a request for a new certificate, or a request to renew a certificate that is about to expire.

ctxcertmgr

A command line tool for managing certificates.

ctxsrvv

A command-line tool for starting up or stopping the server processes on a XenApp for UNIX server.

ctxsrvr

Default member of the Citrix server administrator group.

ctxssl

A special user account for SSL Relay administration. The ctxssl user is part of the Citrix server administrator group account ctxadm. Only the ctxssl user can run the SSL Relay commands and access the SSL Relay directories and files.

ctxsslcfg

A command line tool for configuring SSL Relay.

daemon
A UNIX process that runs in the background for a specific purpose.

denial of service

A security attack in which access to a system or application is prevented or interrupted.

distinguished name

A field in a digital certificate that identifies the issuer of the certificate or the subject of the certificate (such as a XenApp server).

forwarding list

The port numbers and addresses that you permit SSL Relay to redirect to.

hash function

A mathematical representation of information, similar to the checksums found in communication protocols.

identity certificate

A certificate that identifies a subject. There are different types of identity certificate, the most common of which are server certificates and client certificates.

IDS

Intrusion Detection System.

IETF

Internet Engineering Task Force. This organization develop Internet protocol standards.

IIS

Internet Information Server. The Web server built into Microsoft Windows.

integrity

A security service that prevents a message from being modified during its transmission.

IPSec

IP Security. IPSec provides secure communications between the Web server and the XenApp server. IPSec is a standard feature of Microsoft Windows.

issuer

The organization that issued the certificate.

MKS

Microsoft Key Storage. A supported certificate file format.

pass-phrase
A long password used to encrypt the private key.

**PEM**

Privacy Enhanced Mail. A standard for secure email on the Internet. The PEM format is supported by SSL Relay for certificate files.

**period of validity**

A field contained in the digital certificate. The period of validity includes the certificate’s start date and expiry date.

**plaintext**

Non-encrypted information.

**private keys**

One of the keys used in public key cryptography. The private key must be kept secret.

**public keys**

One of the keys used in public key cryptography. The public key can be distributed without compromising security.

**public key cryptography**

A type of cryptography in which one key is used to scramble the message and another key is used to unscramble it. There are always two keys: a public key and a private key. Messages scrambled with one key can only be unscrambled using the other key. Public key cryptography is also known also as Asymmetric Key Cryptography.

**root certificate**

A type of certificate that identifies the CA that signed the server certificate.

**secret key cryptography**

A type of cryptography in which both the sender and the receiver know the same secret key. Messages are scrambled by the sender using the secret key, and unscrambled by the receiver using the same secret key. Secret key cryptography is also known as Symmetric Key Cryptography.

**SecureICA Services**

See Citrix SecureICA Services.

**server certificate**

A type of identity certificate that identifies a specific machine; for example, a XenApp for UNIX server.

**session key**

A cryptographic key used for communication between two parties. The session key is valid for the one session only.
Glossary

SSL

Secure Sockets Layer.

SSL Relay

A Citrix product that provides the ability to secure data communications using the SSL protocol. SSL provides server authentication, encryption of the data stream, and message integrity checks.

symmetric key cryptography

See secret key cryptography.

VeriSign

A public Certificate Authority that provides certificates for public key users. Support for VeriSign root certificates is already built into SSL-enabled plugins and the server running the Web Interface.

Web Interface

The Web Interface is an application portal technology that provides organizations with the ability to integrate and publish interactive applications into any standard Web browser. The Web Interface is a three-tier solution that includes a XenApp server, a Web server, and a client device with a Web browser.

XML Service

The Citrix XML Service communicates information about the applications published in a server farm to the Web server component of the Web Interface deployment. The XML Service for UNIX runs as a daemon on the servers in a server farm.