Administrator's Guide

Version: 9.1
Released: June 2017

Companion Guides:

The UniPrint Infinity High Availability Setup Guide, Cluster Guide, Mobile Setup Guide and Print Route Guide can be found online for your convenience and are intended to assist administrators with the installation and configuration of UniPrint Infinity to reduce printing downtime and enable printing mobility.

- UniPrint High Availability Setup Guide
- UniPrint Cluster Guide
- UniPrint Mobile Setup Guide
- UniPrint Print Route Guide

Revised: 29 March 2018 11:17 am

Disclaimer and Copyright Notice

UniPrint.net Corp. makes no representations or warranties with respect to the contents or use of this publication. UniPrint.net Corp. especially disclaims any expressed or implied warranties, merchantability or fitness for any particular purpose. UniPrint.net Corp. reserves the right to make any changes in specifications and other information contained in this publication without prior notice and without obligation to notify any person or entity of such revisions or changes.

© Copyright 1999 - 2018 UniPrint.net Corp. All rights reserved.

Information in this document is subject to change without notice. Companies, names and data used in examples herein are fictitious unless otherwise noted. Other than printing one copy for personal use, no part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purposes, without the expressed written consent of:

UniPrint.net Corp.
1420-3280 Bloor St. W., Centre Tower
Toronto, Ontario
Canada M8X 2X3
(416) 503-9800
Toll Free: (866) 488-3188 (North America only)
www.uniprint.net

Intellectual Property Acknowledgements

UniPrint and UniPrint Infinity are registered trademarks of UniPrint.net Corp. Registration numbers TMA562,455 and TMA857,027 in Canada and filing number 85-663,579 in the United States. UniPrint.net Corp. products are also registered as United States Patent Numbers 7,064,856, 7,265,867 and 7,602,522.

Microsoft, Windows, Windows 2008/2012/2016, Windows 7/8/10, Microsoft Access, Microsoft Word, Remote Desktop Protocol (RDP), ASP.NET and Active Directory are either registered trademarks or trademarks of Microsoft Corporation.

Citrix, MetaFrame, Presentation Server, XenApp, XenDesktop and ICA (Independent Computing Architecture) are registered trademarks or trademarks of Citrix Systems.

Adobe, Acrobat, Reader are registered trademarks of Adobe Systems Inc.

VMware, Horizon, vMotion are either registered trademarks or trademarks of VMware, Inc.

All other trademarks and registered trademarks are the property of their owners.

Document Revision History

Date	Notes
April 14, 2015	First release.
May 7, 2015	Company name changed to UniPrint.net.
July 2, 2015	Updated to version 9.0.1.
September 23, 2015	Updated to version 9.0.2.
December 14, 2015	Updated to version 9.0.3.
January 26, 2016	Windows Server 2003 SP1 is no longer supported.
February 2, 2016	UniPrint One Queue functionality clarified along with its intentional design use as a guest printing only solution. Therefore, after installation, PrintPAL cannot be used to add additional print queues.
February 9, 2016	Support hours updated.
March 22, 2016	Added instructions on how to remove an associated smart card or proximity ID from the SecurePrint database.
May 17, 2016	Clarified where the UniPrint Adobe Plug-in should be copied in the event of an update for both Adobe Reader and Adobe Acrobat.
June 1, 2016	Updated company name to UniPrint.net Corp.
September 14, 2016	Updated to version 9.0.5. See History.txt for a list of fixes.
November 11, 2016	Updated to version 9.0.6.
February 14, 2017	Updated to version 9.1.
March 27, 2017	Added instructions for installing the Infinity Agent.
April 18, 2017	Added additional parameter for specifying an secondary Bridge during command line installation. Minor corrections regarding the name change from LogScrpt to UPSession.
October 23, 2017	Updated to version 9.1.1.
November 13, 2017	Clarified that the Adobe Plug-in should be always be installed on the Application Server and updated titles on how to print PDFs from Adobe Acrobat and Reader.
March 29, 2018	Removed all instances of the Log file maintenance plug-in since it has been removed from the product.

Table of Contents

Introduction **1**
What is UniPrint Infinity? 1
UniPrint Components 1
UniPrint Bridge 2
UniPrint Print Server 2
UniPrint Application Server 3
Features of UniPrint Infinity 3
Pull-printing with UniPrint VPQ (Virtual Print Queue) 3
Avoid printing related security breaches with SecurePrint 3
Intuitive Installation Package 3
UniPrint Universal Print Driver 4
What's New in Version 9.0 4
High Availability Printing Setup 4
Printer Delegation 4
New Installation Options 5
New Encryption Scheme 5
Version 9.0.1 Updates 5
New file formats supported by Email2Print 5
Version 9.0.2 Updates 5
Support for Windows 10 5
Support for Pass-though in PCoIP 5
Version 9.0.3 Updates 6
Support for the vPad CE 6
Version 9.0.6 Updates 6
vPad CE Web Console 6
Support for VMware Blast Extreme Protocol 6
Local Gateway Queues 6
Version 9.1 Updates 6
Native Printing Support for Mobile Devices Including Chromebooks 6
Support for PC-over-IP (PCoIP) 7
Support for Label Printers (Zebra Printers) 7
Support for Imprivata Authentication 7
Additional Print Job Delegation Functionality 7
Print Route Integration with a New Web Console 7
PrintPAL Verification Tool 7
Infinity Agent For Large VDI Environments 8
Version 9.1.1 Updates 8
User Replacement Mapping for SecurePrint & Email2Print 8
vPad Print Job Filtering 8
SecurePrint Queue Management Through UPSession 8
Option to Use JSON to Populate The PrintPAL Gateway Printer List 8

Installing & Removing UniPrint **9**
Planning Your UniPrint Installation 10
Recommended System Requirements 10
UniPrint Bridge 10
UniPrint Print Server 11

UniPrint Application Server 11
Recommended Minimum Hardware Requirements 12
Disabling Client Printer Mapping on the RDS Server 12
Disabling Automatic Default Printer Management in Windows 10 14
Standard Deployment Scenarios 16
Client/Server Scenario 16
Print Server Scenario 18
VDI Scenario 21
Installing UniPrint Infinity 23
Installing UniPrint Bridge And its Components 23
Installing UniPrint Print Server And its Components 28
Installing UniPrint Application Server And Its Components 32
Installing the Infinity Agent for VDI Environments 38
Installing the Archive Server Component 39
Installing the Statistics Server Component 42
Installing UniPrint from the Command Line 44
Syntax 44
UniPrint Bridge 44
UniPrint Print Server 45
UniPrint Application Server 45
Archive Server 45
Statistics Server 45
Command Line Options 45
/q 45
ADDLOCAL= component 46
INSTALLDIR 48
DOTNETVERSION40CLIENT 48
UP_SETTING_ BRIDGEIP 48
UP_SETTING _RUN_PRINTPAL 49
UP_SETTING_ PAPERSIZE=#n 49
UP_SETTING_ UNIPRINT_AS_ DEFAULT 49
UP_SETTING_ GPO 49
UP_SETTING_ LOGLEVEL=n 50
UP_SETTING_ PASSTHROUGH =#n 50
UP_SETTING_ NO_UNIPRINT_ PRINTER 50
UP_SETTING_ NO_SAVE_QUEUE 51
UP_SETTING_ VC_ORDER 51
USE_VDI_SERVER_SETTINGS 51
UP_SETTING_ STAT_SERVICE_ PORT 51
UP_SETTING_ STAT_CLIENT_ PORT 52
Using Group Policy to Deploy UniPrint Remotely 52
Modifying & Removing UniPrint 58
Modifying a UniPrint Installation 58
Removing UniPrint 59

Configuring UniPrint Bridge 61
Obtaining and Applying a UniPrint Infinity License 61
Obtaining a UniPrint License 61
Applying a UniPrint License 64

Viewing and Saving a Snapshot of License Usage 66
Viewing a Snapshot of License Usage 66
Saving a License Usage Snapshot To a File 68
Copying a License Usage Snapshot to the Clipboard 71
Setting License Thresholds & Alerts 72
Enabling Licensing Alerts 72
Changing Licensing Alerts Frequency 73
Setting the License Threshold 74
Creating a Task to Send an E-mail When An Exceeded Threshold Event is Triggered ..76
Searching For A Particular Printer 80
Changing Default Printer Properties for Gateway Printers Globally For All Users 83
Adding a Lexmark/HP FTP Printer 86
Deleting a Gateway Printer from the UniPrint Bridge 90
Enabling PDL Support for Label Printers 92

Configuring UniPrint Print Server 95
Adding a Gateway printer 95
Re-publishing a Printer to the UniPrint Bridge 97
Changing How Gateway Printers are Published to the UniPrint Bridge 100
Setting Default Printer Properties for New & Republished Gateway Queues 103
Enabling Font Replication 106
Configuring Printer Profiles 108
Creating a New Printer Profile 109
Editing an Existing Printer Profile 114
Deleting a Printer Profile 116

Configuring UniPrint Application Server 119
Preparing UniPrint for Custom Forms 119
Defining a custom Form on the Application (Citrix/RDS) Server 119
Using a Custom Form in a User Session 121
Defining a Custom Form in a User Session 123
Changing UniPrint Printer Properties Globally For All Users 124
Copying UniPrint Printer Properties to Another Application Server 127
Enabling & Configuring UniPrint To E-mail Print Jobs as PDF Attachments 129
Enabling UniPrint To Save Print Jobs As PDF Files 132
Enabling & Setting Order of Precedence of Group Policy Objects 133
Enabling Policies 133
Forcing UniPrint Infinity to Apply Settings Only From The Management Console 136
Changing the Order of Precedence 137
Enabling Applications to Save User Settings With UPSession 139
Enabling UniPrint Session Features 140
Setting Which Protocols Are Used To Transfer Print Jobs To The UniPrint Client 140
Changing the Order That UniPrint Infinity Uses For Auto-detecting Transfer Protocols .. 141
Setting This Application Server As A Pass-through Client 143
Setting Session Logon Features 144
Configuring UniPrint Adobe Plug-in 146
Replacing the Print function with Print to UniPrint 146
Enabling the UniPrint Adobe Plug-in to run with Adobe Reader XI & Later 147

Whitelisting the UniPrint Adobe Plug-in 147
Disabling Protected Mode at Startup in Adobe Reader XI & Later 148
Previewing PDF Documents With Adobe Reader 150
Using Adobe Reader to Preview PDF Print Jobs 151
Creating Multiple UniPrint Printer Queues 153
Changing the Number of Allowable UniPrint Queues 153
Creating Another UniPrint Printer Queue 154

Configuring UniPrint Using ADMs & ADMXs 157
Loading a Classic Administrative Template 157
Loading and Configuring an Administrative Template in Windows Vista or later 161

Configuring PrintPAL 165
Planning Your PrintPAL Mapping 165
Setting Initial PrintPAL Configuration Settings 166
Creating Groups for the PrintPAL Map 170
Adding A Device to the PrintPAL Map 171
Adding an IP Range of Objects to the PrintPAL Map 173
Mapping Network Objects to a Group in PrintPAL 175
Mapping Printers to a Group in PrintPAL 180
Setting Default Printers in PrintPAL 182
Enabling Local Gateway Queues in PrintPAL 184
Testing Your PrintPAL Map 187
How PrintPAL Determines Which Printers to Map 187
Testing By Device Name, IP Address or User Name 189
Testing A Current Session 191
Setting PrintPAL To Automatically Map Printers When A Session Is Started 195
Setting PrintPAL To Delete and Then Remap Printers in a Session 196
Setting PrintPAL Communication to Use JSON 197
Discovering Orphaned Printers and Printers With Offline Status 198

Configuring SecurePrint 201
Configuring UniPrint SecurePrint 201
Installing the UniPrint vPad Device 201
Installing the vPad CE Device 202
Installing the vPad CE2 Device 203
Running the SecurePrint Emulator 204
Activating the UniPrint vPad 204
Configuring the vPad CE to Connect to the UniPrint Print Server 208
Using SecurePrint.ini on a USB Flash Drive 208
Using the vPad CE Web Interface 212
Troubleshooting: vPad Pro/CE Cannot Connect to the UniPrint Print Server 214
Organizing Your vPads Using Folders 221
Changing SecurePrint Settings for A Single vPad Device 224
Changing SecurePrint Settings Globally for All vPad Devices 226
Adding Printers to the vPad 233
Deleting a Printer from a vPad 236
Disabling the Force Password option on a printer 237
Associating A Smart Card With A User Name 238

Disabling and Removing an Associated Smart Card From SecurePrint 239
Importing A List Of Users and Smart Card IDs Into SecurePrint 242
Associating Many E-mail Addresses to One Domain User Name 246
Importing a List of E-mail Addresses and User Names 250
Limiting The Number Of Printers Viewed On The vPad 255
Enabling Users To Print All Jobs With A Single Swipe Of Their Card 259
vPad Print Job Filtering 260
Example Usage Scenario 260
Enabling Data Compression Between Print Server And Printer Through The vPad 261
Viewing Compression Statistics 264
Troubleshooting Print Stream Compression 265
Setting up Imprivata OneSign for SecurePrint Authentication 266
Installing the Imprivata Gateway Component 266
Integrating UniPrint Infinity on the Imprivata OneSign Server 267
Configuring SecurePrint to Recognize Imprivata OneSign 267
Configuring The UniPrint vPad Device 270
Adjusting Screen Brightness and Backlighting 271
Setting Up A Screensaver 272
Changing the Default Home Page & Refresh To Home Page 274
Changing Print Server Connection Information 276
Assigning a Static IP Address To The vPad Pro 279
Changing the Number of Users Listed Under Recently Searched User Names 282
Changing the Interface Language 284
Adjusting Sound and Volume 287
Muting Tap Sounds 288
Retrieving Information About the vPad 289
Configuring Printer Delegation 291
Setting up Email Server Settings for Printer Delegation 292
Creating a New Delegate Printer Queue 293
Assigning Delegates and vPads to a Delegate Printer Queue 294
Modifying a Delegate Printer 297
Republishing a Delegate Printer to the Bridge 298
Deleting a User or vPad From The Delegates List 299
Deleting a Delegate Printer Queue 300
Delegating a Print Job 300
Printing through the vPad CE 303
Setting up your SecurePrint Password 304
Resetting your SecurePrint Password 306
Managing the SecurePrint Queue Within a User's Session 307
Retrieving Your Document Through the vPad Device 308
Retrieving a Delegated Print Job 314

Configuring Print Job Archiving 319
Deployment Scenarios 319
Standard Deployment 320
Custom Deployment 321
Changing the Archive Location 321
Restricting When Print Jobs Are Archived 323

Retrieving Print Job Statistics 327
Deployment Scenario 327
Standard Deployment 328
Retrieving Print Job Data From The Statistics Server 328

Printing with UniPrint Infinity 335
Adding a UniPrint Gateway Printer 335
Adding a Gateway Printer Manually 336
Adding a Gateway Printer Using PrintPAL And UPSession 338
Adding a Gateway Printer Using the One Queue (Session Login Not Required) 340
Sending Printed Documents as E-mail Attachments 344
Saving Printed Documents as PDF Files 350
Using Printer Profiles to Print With Advanced Printer Properties 355
Printing PDFs from Adobe Acrobat or Reader 358
Printing PDFs from Adobe Acrobat or Reader 9 358
Printing PDFs from Acrobat or Reader X or XI 359
Printing PDFs from Acrobat Reader DC or later 362
Disabling Pop-up Messages When Not Logged In 365

Contact and Support 367
UniPrint Support 367
North America 367
Europe, Middle East and Africa 367
E-mail 367
Office Location 367
Address 367

Addendum A: UniPrint Management Console Interface 369
Console Home 370
Properties & Settings 372
Printers 372
SecurePrint 373
Default Settings 374
Users/Cards View 380
Components 380
UniPrint Printer Driver 381
SecurePrint Server 381
PrintPAL Server 381
UniPrint Session Application 381
Archive Client 382
UniPrint Control Service 382
Active Directory console processor 383
Active Directory Processor 383
Alternate Server Plugin 383
Archive Server 383
Bridge server info processor 384
Connected node management plug-in 384
Document conversion processor 384
Email2Print Server 385

Font replication plug-in 385
Font request processor 385
FTP print job processor 385
License manager plug-in 386
License request processor 386
Management console connector 386
Management console HTTP server to enable web-based administration 386
Node identification plug-in 386
Node request processor 386
Print Job storage processor 387
Print job processor 387
Printer change monitor 387
Printer creation processor 388
Printer discovery plug-in 388
Printer discovery plug-in (Bridge) 388
Printer lookup optimization plug-in 388
Printer settings synchronization processor 389
PrintPAL Server Relay 389
PrintPAL Settings Syncing Plugin 389
Process delegation plug-in 389
Profile discovery plug-in 390
Quorum synchronization plug-in 390
Remote Console query processor 390
SecurePrint Job processor 390
UniPrint Bridge 64-bit layer plug-in 390
UniPrint Bridge service discovery plug-in 390
UniPrint compressed Printstream relay server 391
UniPrint Data Server 391
UniPrint driver install plug-in 391
UniPrint vPAD device relay server 391
UniPrint printer install plug-in 391
UniPrint SecurePrint & VPQ server 391
UniPrint IPP Service 392
UniPrint Bridge Service 392
Discovery mode 392
Locked Down 392
Other Log Files 392
UPStatSvc_%timestamp%.log 393
UPStatClientSvc_%timestamp% .log 393
UPPrintPALCacheSvr_%timestamp%.log 393
UPImprivataSvr_%timestamp%.log 393
UPAUXSvc_%timestamp%.log 393
UPDeviceHTTPSSvr_%timestamp%.log 393
UPChromeSvc_%timestamp%.log 393
Policies 394
User policy 394
Machine policy 394
User settings 394
Machine settings 395

Network Connections 395
Sessions (UniPrint Application Server only) 395
Protocols 395
Pass-through 396
Logon options 396
Wait for Userinit to finish 396
Set UniPrint as default printer 396
Delete leftover print jobs 396
Run PrintPAL on this server 396
Services 397
UniPrint Control Service 397
Connected node management plug-in 397
Document conversion processor 397
License manager plug-in 397
Print job processor 397
Printer change monitor 398
UniPrint compressed Printstream relay server 398
UniPrint Data Server 398
UniPrint vPad device relay server 398
UniPrint Remote Console Listener 398
UniPrint SecurePrint & VPQ server 398
UniPrint Bridge Service 398
UniPrint IPP Service 398
Tools & Utilities 399
Database Configuration 399
PrintPAL 400
Group Map 401
Mapped Objects/Criteria 401
Mapped Printers 401
Mappable Objects & Printers 401
Printer Profiles (UniPrint Print Server Only) 402

Addendum B: Gateway Printer Properties Interface 403
General Tab 403
Paper Size 403
Orientation 404
Paper 404
Resolution 404
Source 404
Double Sided Printing 404
Flip pages up 404
Flip pages sideways 404
Color 404
Grayscale 404
Color 405
Advanced Tab 405
Font Embedding Options 405
No font 405
Full font 405

Minimal font 405
Standard fonts 406
Licensed fonts 406
Language fonts 406
Emulation 406
PostScript 406
Physical margins (mm) 406
Horizontal 406
Vertical 406
Resizing Options 406
Scale to fit 406
% of actual size 406
Multi-pages per sheet 407
Preview document with a PDF viewer 407
Image Settings Button 407
Black & White Compression 407
Default compression 407
CCITT Fax Group 4 408
Color Compression 408
Default compression 408
256 color compression 408
JPEG compression 408
Automatic 409
Remove duplicated images 409
SecurePrint Tab 409
Print Handling Tab 410
Available profiles 410
Document Handling 411
Auto Center 411
Fit To Page 411
About Tab 411

Addendum C: vPad Console Interface 413
Console Home 413
Settings 414
Screen 415
Backlight 415
Auto adjust backlight 415
Brightness 415
Screensaver theme 416
Advanced 416
Home page 417
Auto show home page 417
Server connection mode 417
Configure ethernet 418
Recently searched list 418
Language 419
Sound 419
Audible selection 419

Volume level 419
Information 420
Recent User List 420
Pending Print Jobs User List 421
Printer Settings 422
Profile 422

Addendum D: Paper Sizes 425

CHAPTER 1

UniPrint Infinity

Introduction

What is UniPrint Infinity?

UniPrint Infinity is a comprehensive printing solution for Server-based Computing (SbC), virtual desktop infrastructure (VDI) and secure mobile printing. The UniPrint Infinity solution provides users with the flexibility to print to any type of device from a Citrix and/or Remote Desktop Services session, or from any mobile device with the additional benefits of Portable Document Format (PDF).

With UniPrint Infinity printing to network or local printers, USB printers or even specialized devices, are all performed by a single universal printer driver, which eliminates extra configuration and confusing options for users. UniPrint Infinity supports Citrix and Microsoft Remote Desktop Services, and VDI architectures.

UniPrint Infinity supports many different endpoints including desktops, thin-clients and zero clients printing from ICA/RDP sessions or printing from a virtual desktop image in VDI environments and mobile devices such as smartphones, tablets, Chromebooks and laptops.

Printing from mobile devices is also supported with UniPrint Mobile Printing, the AirPrint Printing Module, and Email2Print.

UniPrint Components

There are three main components that make up a typical UniPrint Infinity deployment - the UniPrint Bridge, the UniPrint Print Server and the UniPrint Application Server. It is important to note that not all UniPrint components need to be installed. Which UniPrint component is installed, and where it is installed, depends on which UniPrint deployment scenario is chosen. Below is description of each key UniPrint component. For more information, see "Standard Deployment Scenarios" on page 16.

UniPrint Bridge

The UniPrint Bridge acts as a communication router and is required in all deployment scenarios. By default, the license server component is also installed on the UniPrint Bridge. The license server component validates UniPrint licenses when each UniPrint Application Server machine connects. PrintPAL is also installed by default and is used to automate printer to user session mapping. UniPrint Bridge is typically installed first, since connectivity can be verified among the remaining components, UniPrint Print Server and UniPrint Application Server.

The following components can also be installed on the UniPrint Bridge:

- SecurePrint Server & Data Server – For secure pull printing and print stream compression
- UniPrint Mobile Server – For mobile printing from Android, iOS, and Chrome OS devices
- Imprivata Gateway – For user authentication through Imprivata instead of through SecurePrint.

UniPrint Print Server

UniPrint Print Server is responsible for rendering print jobs and directing them to the appropriate printer.

In enterprises where users are located in different geographic regions or where printing requirements vary greatly from branch office to branch office, UniPrint Print Servers are typically located in the same location as the printers themselves. Deploying multiple UniPrint Print Servers has several advantages:

- It distributes the printing workload between remote locations.
- It accommodates differences in regional printing environments.
- It reduces bandwidth consumption by transferring compressed PDF files instead of RAW data files across the network.

However, if Print Server consolidation is important then UniPrint Print Servers can also be housed in a central location such as a data center. In this case, Print Stream Compression is highly recommended to reduce the amount of RAW print data being sent across the WAN to the remote location. By using Print Stream Compression in combination with SecurePrint, the vPad Pro or CE can replace the remote print server and decompress the print stream before forwarding the print job to the printer.

Server/client environments have the option not to install UniPrint Print Server and install UniPrint Client on their workstations instead.

UniPrint Application Server

UniPrint Application Server consists of the UniPrint universal printer driver and is responsible for rendering server-based print jobs to compressed PDF files. This component is installed on a Citrix or Remote Desktop server. For a VDI environment, UniPrint Application Server is installed on the golden image.

Features of UniPrint Infinity

Pull-printing with UniPrint VPQ (Virtual Print Queue)

With UniPrint VPQ pull-printing has never been easier. Users need not worry about selecting a printer until they authenticate using the UniPrint vPad (user authentication device) or SecurePrint emulator. They can simply send all of their print jobs to the UniPrint VPQ. Later, when they have a spare moment, all they need to do is authenticate, and then select a printer to output their documents.

Avoid printing related security breaches with SecurePrint

In combination with the UniPrint vPad (user authentication device) or SecurePrint emulator, SecurePrint will not release print jobs until the user has authenticated. SecurePrint eliminates unclaimed printed documents thus avoiding potential security breaches and reducing paper waste.

The UniPrint vPad easily connects to any wired network and is printer make and model independent. The vPad not only supports password authentication, but also supports smart cards (both contact and contactless), magnetic stripe, RFID, and most HID cards (depends on the HID version).

SecurePrint can also be integrated with Active Directory to restrict user access to certain printers. With UniPrint Print Guard, only the permissible printers will be displayed to the user on the vPad.

Intuitive Installation Package

The installation package allows UniPrint components to be installed in many different configurations. This empowers Network Administrators to install UniPrint in any way that they see fit for their environment. However, this Administrator's Guide describes best practise scenarios for deployment. For example, the License Server component can be installed on any server.

UniPrint Universal Print Driver

The streamlined UniPrint driver not only allows the user to e-mail and save their print jobs as PDF files, but the user can also encrypt and password protect these PDF files. This added security ensures that only the intended user can open, modify and print the PDF files created with UniPrint.

What's New in Version 9.0

UniPrint Infinity supports printing from mobile devices through its AirPrint Printing Module and Email2Print. With the AirPrint Printing Module, printers on the print server and the VPQ are made Apple-compatible for Apple devices connected to your corporate network.

Email2Print enables users to e-mail a PDF document as an attachment to an e-mail address that is designated to a printer and the PDF document then prints out at that printer. Other document and file types will be supported in the near future.

These add-on modules are sold separately but are fully compatible with UniPrint Infinity. The UniPrint Infinity Mobile Setup Guide is available as a separate document.

High Availability Printing Setup

UniPrint Infinity can be set up such that printing downtime is a thing of the past. Through the high availability (HA) setup, should a UniPrint Bridge or UniPrint Print Server fail, functionality will immediately fail over to the inactive Bridge or Print Server. This setup is an alternative to Microsoft Cluster Services.

Since separate HA licenses are required, a separate High Availability Setup Guide is available.

Printer Delegation

This new SecurePrint feature allows users to send an e-mail notification with a PIN code to a group of users. This negates having to send confidential documents as e-mail attachments and instead allows recipients to securely print out these documents by entering the randomly generated PIN code at the vPad device.

New Installation Options

One Queue Mapped to Install allows users to map to a Gateway printer queue, which then installs UniPrint core components such as the UniPrint driver, UPSession (formerly LogScrpt) and the UniPrint Control Service without having to install the UniPrint Application Server on their machines. This installation option is only intended for guests who need to print to a network printer, but don't want to install UniPrint Application Server on their machines.

For VDI setups, during the installation of the UniPrint Application Server, administrators now have the option not to make the connection to the UniPrint Bridge static. A connection to the UniPrint Bridge will only be established when the user prints. Administrators also have the option not to install the UniPrint Management Console on the golden image.

New Encryption Scheme

In this version the old 48-bit encryption scheme has been replaced with a new 256-bit encryption scheme.

Version 9.0.1 Updates

New file formats supported by Email2Print

Email2Print now supports many different file formats, including Microsoft Office files, graphics files and PDF. For a full list of supported file formats, refer to the UniPrint Infinity Mobile Setup Guide.

Version 9.0.2 Updates

Support for Windows 10

Version 9.0.2 now supports Windows 10. The UniPrint Print Server component can also be installed on Windows 10.

Support for Pass-though in PCoIP

Nested PCoIP sessions are now support in this update.

Version 9.0.3 Updates

Support for the vPad CE

The vPad CE is a small printing appliance and unlike the vPad device, the vPad CE does not come with a "pad" or any form of user input and display. This device comes with 4 USB ports and an Ethernet port.

The purpose of the vPad CE is to help consolidate print servers and facilitate print stream compression for remote printing. Print jobs processed through UniPrint Infinity will be compressed on the print server, transmitted to and decompressed by the vPad CE, before being routed to the appropriate remote printer for printing. The vPad CE can support up to 5 concurrent print jobs at a time.

Version 9.0.6 Updates

vPad CE Web Console

For simple configuration of the vPad CE device, the vPad CE web console can be used to change various settings with ease.

Support for VMware Blast Extreme Protocol

Version 9.0.6 now supports VMware Blast Extreme protocol which improves latency, bandwidth conservation and CPU usage.

Local Gateway Queues

Without requiring the Windows File and Printer Sharing ports to be open to the internet, local Gateway queues enable users who log into Application Servers that are not part of their domain to print to a Gateway printer queue. This Gateway printer queue will appear as a local print queue in the user's session. Local Gateway queues are enabled through PrintPAL in the UniPrint Management Console

Version 9.1 Updates

Native Printing Support for Mobile Devices Including Chromebooks

This latest version of UniPrint Infinity, now supports native printing from Android, iOS, and Chrome OS. Smartphones, tablets, and Chromebooks can now print natively and securely to corporate printers without going through the cloud or registering through a third party cloud service.

Mobile Printing easily integrates with SecurePrint, to ensure print jobs sent from a mobile device are not left on the printer. This avoids possible security breaches and saves paper and ink wastage. For more information on setting up and using UniPrint Infinity Mobile Printing, refer to the UniPrint Infinity Mobile Setup Guide.

Support for PC-over-IP (PCoIP)

UniPrint Infinity now fully supports PCoIP as a transfer protocol.

Support for Label Printers (Zebra Printers)

Some label printers use Page Description Language (PDL) to print and converting print jobs for these printers to PDF was problematic in the past. With this release, PDL support is included and allows ASCII text to print properly and accurately to the label printer without conversion to PDF format.

Support for Imprivata Authentication

For organizations that already have Imprivata implemented, UniPrint Infinity now supports Imprivata authentication for SecurePrint which allows users to use their Imprivata proximity card to authenticate themselves to release print jobs.

Additional Print Job Delegation Functionality

Along with delegating print jobs to specific users, print jobs can also be delegated to specific vPads. This ensures that the delegated print job is only printed out at certain printers.

Print Route Integration with a New Web Console

With Print Route, administrators can assign a local print queue to a Gateway print queue for a specific set of devices. Print Route is now integrated into UniPrint Infinity and configuration is now done through a new Web Console, which can be accessed from any location. For detailed instructions on setting up and using Print Route, refer to the Print Route Utility Guide.

PrintPAL Verification Tool

For large print environments that are constantly changing, it is easy to lose track of decommissioned printers and keep track printers in PrintPAL. The PrintPAL Verification tool examines the entire PrintPAL map looking for orphaned printers and reports back the groups that are affected. The

administrator can then review the report and take action on the orphaned printers.

Infinity Agent For Large VDI Environments

To help expedite deployment of UniPrint Infinity 9.1, an installation agent is available to install on virtual desktop images. This agent will install the UniPrint Application Server component without the Management Console. The No static connection to the Bridge Server option and PrintPAL will also be enabled. The Infinity Agent can be downloaded at https://www.uniprint.net/members/download/agent/InfinityAgentInstaller911.exe.

Version 9.1.1 Updates

User Replacement Mapping for SecurePrint & Email2Print

User Replacement Mapping allows users with multiple e-mail addresses to print through Email2Print and then view those print jobs through the vPad under a single domain user name. This one user name to many e-mail addresses feature simplifies user workflow on the vPad, since users no longer need to enter individual email addresses to release their print jobs. They only need to enter their domain user name and all of their Email2Print and session print jobs will be listed.

vPad Print Job Filtering

When using the Print all on card swipe option, an administrator can set up a filter that will allow certain print jobs to print based on a specified regular expression. For example, if a user prints several jobs, the print jobs with the word "Label" in the file name can be filtered such that they only print to label printers when the user taps their RFID/HID card at the vPad.

SecurePrint Queue Management Through UPSession

This enhancement enables users who forget their SecurePrint password, the ability to view their list of SecurePrint print jobs and delete them. This function is disabled by default.

Option to Use JSON to Populate The PrintPAL Gateway Printer List

For large print environments, PrintPAL can be populated with Gateway printers faster and the network traffic greatly reduced, if communication is changed to JSON. This enhancement is approximately 50% faster than our default method and is more noticeable when the environment contains hundreds of printers. This enhancement is disabled by default.

CHAPTER 2

UniPrint Infinity

Installing & Removing UniPrint

UniPrint Infinity comprises of three main components: UniPrint Bridge, UniPrint Print Server, and UniPrint Application Server. All three components are installed using the same installer. However, the installer needs to be run separately on each server machine.

Other UniPrint components to consider include the following:

- License Server, of which only one instance can exist in the environment, with the exception of a high availability deployment where two instances are required. By default, the License Server is installed with the UniPrint Bridge. However, the License Server does not necessarily need to be installed on same server as the UniPrint Bridge.
- SecurePrint Server and SecurePrint Data Store are required if the vPad, SecurePrint emulator or Print Stream Compression are being deployed. These are also packaged with the UniPrint Bridge. The SecurePrint print server components are also required and they are packaged with the UniPrint Print Server.
- Archive Server and Archive Client are used to automatically archive print jobs as PDF files, and can be used to archive print jobs sent to Gateway printers, the UniPrint VPQ and to the UniPrint printer. Each time a user prints, the print job is automatically archived to the location specified in the UniPrint Management Console.
- Statistics Server and Statistics Client are used to monitor print job statistics for Gateway printers, the UniPrint VPQ, the UniPrint printer, the UniPrint (Email PDF) queue and the UniPrint (Save PDF) queues. Statistics such as number of pages, color or black & white, user, print queue name, etc. are captured on the Statistics Server. Print job statistics can be displayed in report format using the Statistics Viewer. This free utility can be downloaded from https://www.uniprint.net/eng/page/download-tools-and-utilities.
- PrintPAL Server is used to automatically map printers to sessions based on devices, IP ranges, users, user groups, and organizational units. PrintPAL Server is packaged with the UniPrint Bridge.

- Adobe Plug-in is for users who print documents that are already in PDF format. This is packaged with the UniPrint Application Server.

NOTE: Upgrading to UniPrint Infinity 9.1 is not supported. In order to "upgrade" to version 9.1, a complete removal of the previous version of UniPrint and then a brand new installation of version 9.1 is required. Before removing the previous version, run the Backup and Restore utility first to back up key UniPrint configuration settings and restore it to a version 9.1 deployment. To obtain a copy of the Backup and Restore utility, contact UniPrint Support.

- Printer Delegation is a SecurePrint module that enables users to send an email notification with a PIN code to a group of users to allow them to print a delegated print job. This negates having to send confidential documents as e-mail attachments to a group of users and instead allows recipients to securely print out these documents by entering the randomly generated PIN code at the vPad device. Delegated print jobs can be further restricted to only be released at a specified vPad device.

Mobile Printing Solutions include the following:

- UniPrint Mobile Printing allows Android, iOS, and Chrome OS devices to print natively to any printer in the corporate print environment.
- Email2Print allows smartphone, tablet and laptop users to send documents as attachments to an e-mail address that is associated with a particular printer in order to print.
- The AirPrint Printing Module converts any printer on your print server into an Apple-compatible printer thereby allowing any iPad, iPhone or MacBook device to print directly to these printers.

Planning Your UniPrint Installation

Recommended System Requirements

To ensure the installation of UniPrint Infinity is successful, ensure that your servers meet the recommended system requirements for each UniPrint component.

UniPrint Bridge

The UniPrint Bridge requires one of the following supported operating systems and all of the roles and features listed:

- Microsoft Windows Server 2008 or R2
- Microsoft Windows Server 2012 or R2
- Microsoft Windows Server 2016

- with .NET Framework 4.5 feature installed

UniPrint Print Server

The UniPrint Print Server requires one of the following supported operating systems and all of the roles and features listed:

- Microsoft Windows 7
- Microsoft Windows 8/8.1
- Microsoft Windows 10
- Microsoft Windows Server 2008 or R2
- Microsoft Windows Server 2012 or R2
- Microsoft Windows Server 2016
- with .NET Framework 4.5 feature installed

UniPrint Application Server

The UniPrint Application Server requires one of the following supported operating systems and all of the roles and features listed:

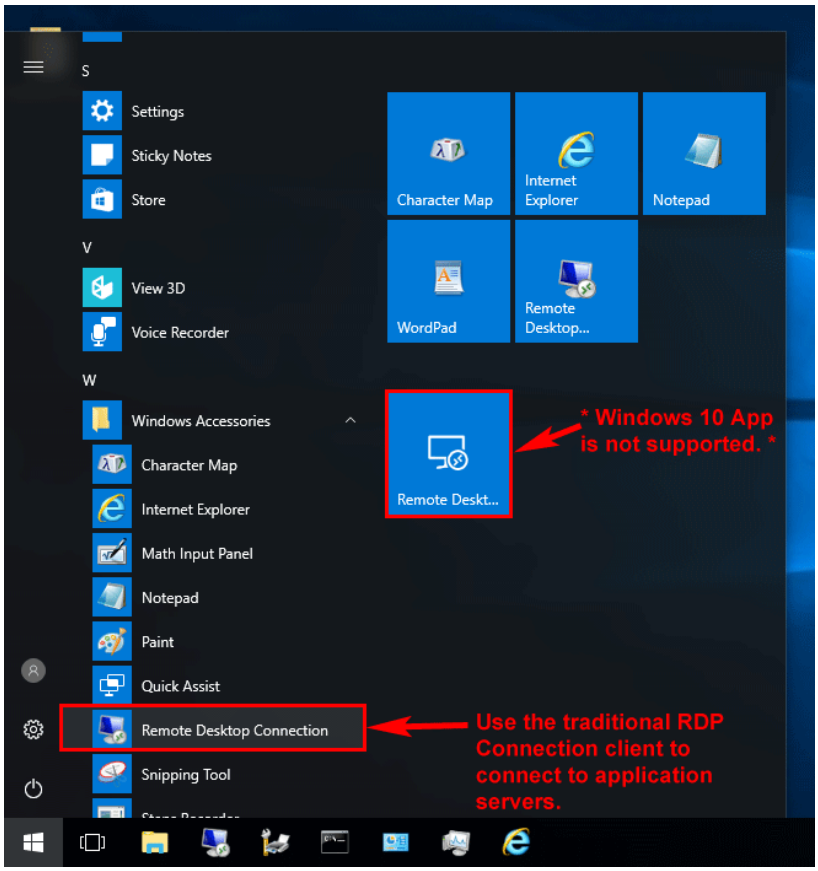
- Microsoft Windows Server 2008 or R2
- Microsoft Windows Server 2012 or R2
- Microsoft Windows Server 2016
- with Remote Desktop Services role installed
- with .NET Framework 4.5 feature installed

In a VDI environment, UniPrint Application Server is installed on each golden image with one of the following supported operating systems with all of the roles and features listed:

- Microsoft Windows 7 (***Note**: Windows 7 Starter, Home Basic and Home Premium are NOT supported because these versions do not support Remote Desktop Services*.)
- Microsoft Windows 8 or later
- Microsoft Windows 10

- with .NET Framework 4.5 feature installed

NOTE: The new Windows 10 Remote Desktop app is not supported. RDP users are required to connect to their application servers using the traditional RDP client.



Recommended Minimum Hardware Requirements

For both the UniPrint Bridge and UniPrint Print Server, the recommended minimum hardware requirements are as follows:

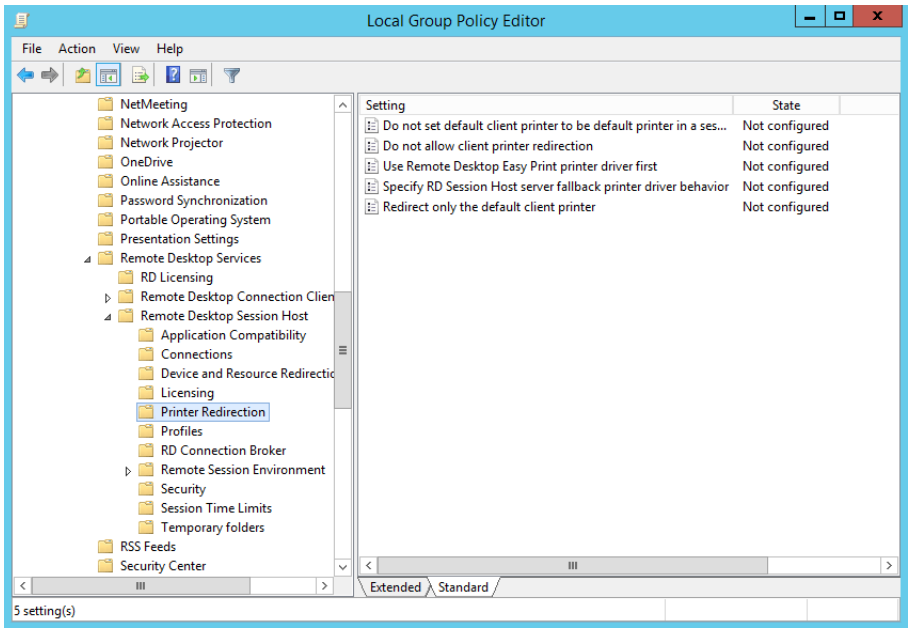
- 8GB RAM
- A quad core processor
- At least 100GB free disk space.

Disabling Client Printer Mapping on the RDS Server

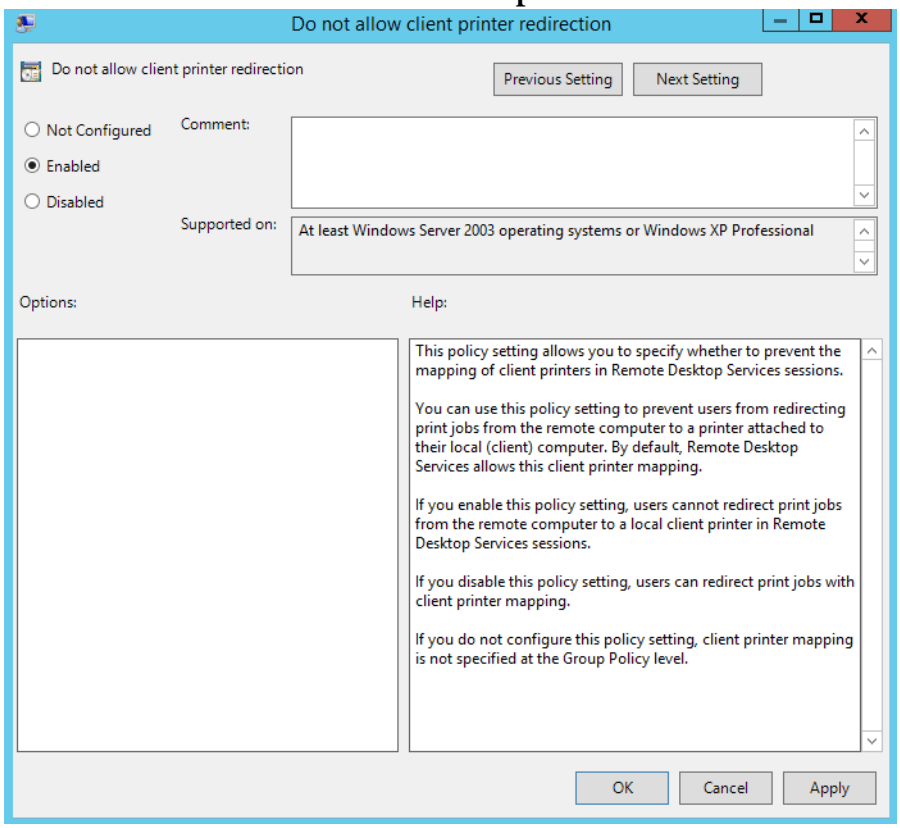
Prior to deploying UniPrint Infinity, it is highly recommended that client printer mapping be disabled on the RDS server. In Windows Server 2012 R2, this can be accomplished through Group Policy Objects.

1. On the Application Server, click **Run**, type `gpedit.msc` and then click **OK**.

2. In the console tree, under **Computer Configuration**, expand **Administrative Templates**, **Windows Components**, **Remote Desktop Services**, **Remote Desktop Session Host**, and then **Printer Redirection**.



3. Double-click **Do not allow client printer redirection**.



4. Select **Enable**. Click **Apply** and then click **OK**.

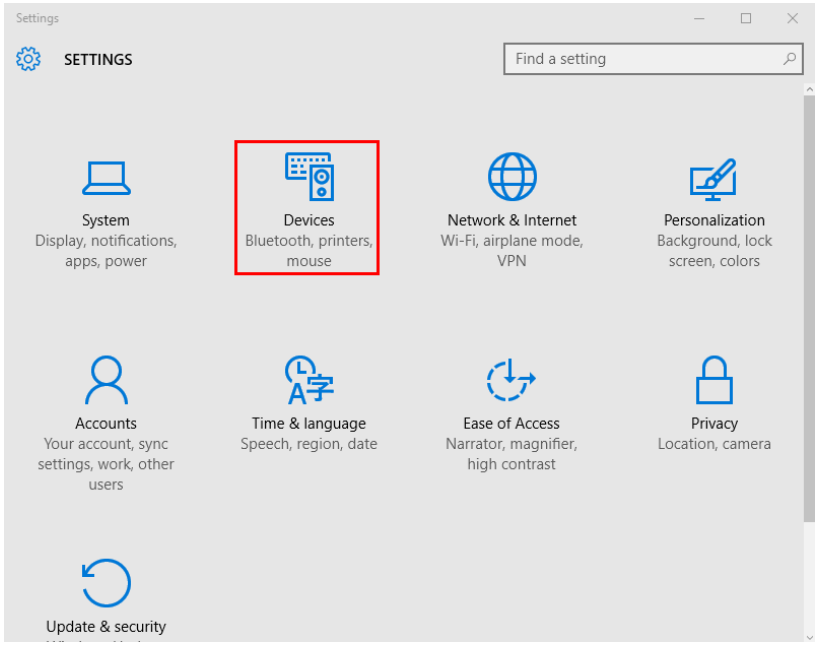
Disabling Automatic Default Printer Management in Windows 10

Before deploying UniPrint Infinity, it is highly recommended that **Automatic Default Printer Management** on Windows 10 Build 1511 and later workstations be disabled. This is especially necessary for PrintPAL mapping to work properly.

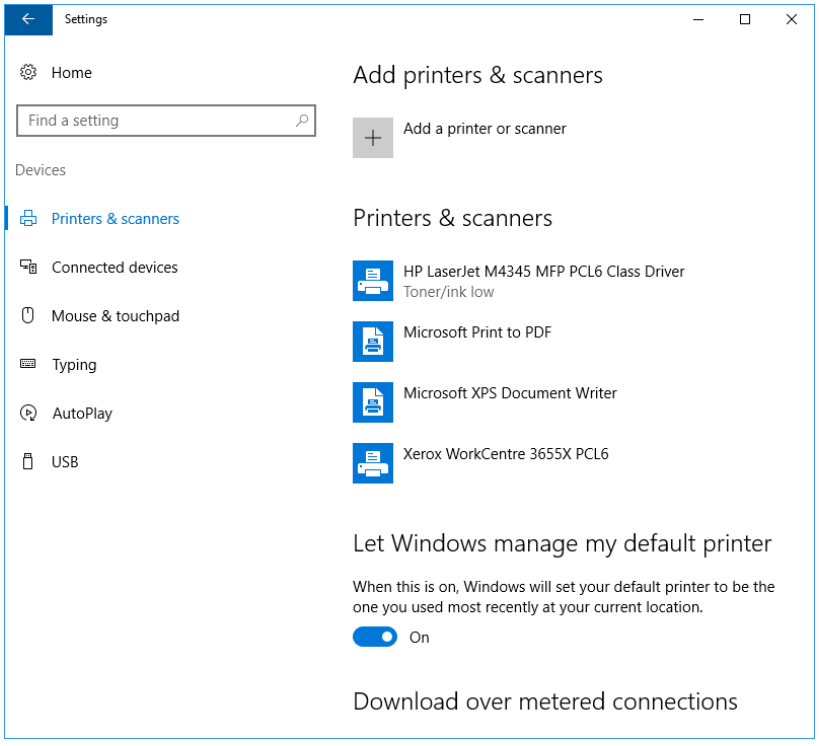
To disable automatic default printer management, do the following:

1. In Windows 10, click **Start** and then open **Settings**.

2. Click **Devices**.



3. By default, **Let Windows manage my default printer** is **On**. Click to toggle this setting to **Off**.



Standard Deployment Scenarios

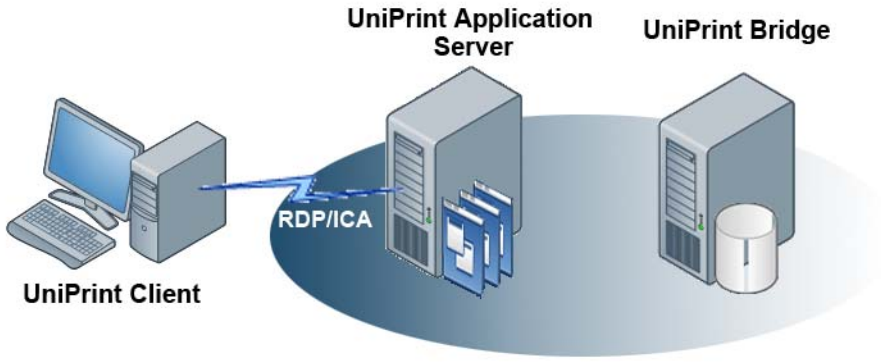
UniPrint Infinity can be deployed in many different environments which includes the following:

- An environment in which the client endpoints have accessible hard drives, connect to application servers through RDP/ICA, herein called the Client/Server scenario.
- An environment in which client endpoints with inaccessible hard drives connect to application servers through RDP/ICA, herein called the Print Server scenario, since a print server is required to process print jobs on behalf of the client endpoint in this type of environment.
- An environment in which client endpoints, including zero clients, access and print through virtual desktop images, herein called the VDI scenario.

Where to install the various UniPrint components depends on the type of scenario that best fits your particular IT infrastructure, the type of client endpoints, and user requirements.

Before installing UniPrint Infinity, ensure that client printer redirection is disabled on the remote desktop server. For instructions, see "Disabling Client Printer Mapping on the RDS Server" on page 12.

Client/Server Scenario



In this scenario, workstation users print from Remote Desktop or Citrix sessions. The connecting desktop machines must have accessible hard drives. Three components are required to be installed on two servers and on at least

one desktop machine -- UniPrint Bridge with the License Server, UniPrint Application Server and the UniPrint Client on the desktop machine.

The recommended installation order for a Client/Server deployment, is as follows:

1. Install **UniPrint Bridge** on a server. ***Note**: The **UniPrint License Server** component is packaged with the UniPrint Bridge installation file. The UniPrint License Server does not necessarily have to be installed on the same server as the UniPrint Bridge, but only one instance of the UniPrint License Server can exist in your UniPrint Infjnity deployment.*

2. Install **UniPrint Application Server** on a Remote Desktop/Citrix server. If Adobe Reader or Acrobat is already installed, then the **Adobe Plug-in** is installed by default.

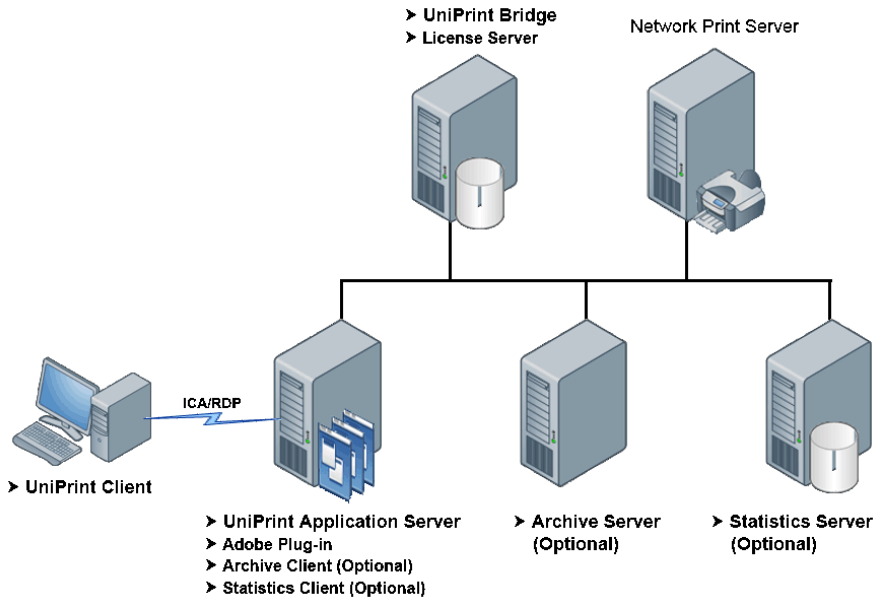
NOTE: It is **HIGHLY RECOMMENDED** that the Adobe Plug-in be installed since it prevents UniPrint from re-rendering PDFs. Re-rendered PDFs often results in replaced or missing fonts and sometimes the re-rendered PDF size can be much larger than the original file size if the Adobe Plug-in is not used. The Adobe Plug-in should always be installed unless it is known for sure that users will not be printing PDFs from Adobe Reader or Acrobat.

OPTIONAL: If print job archiving is being deployed, install the **Archive Client** on the same server machine as UniPrint Application Server and also install the **Archive Server** on a separate, independent file storage machine.

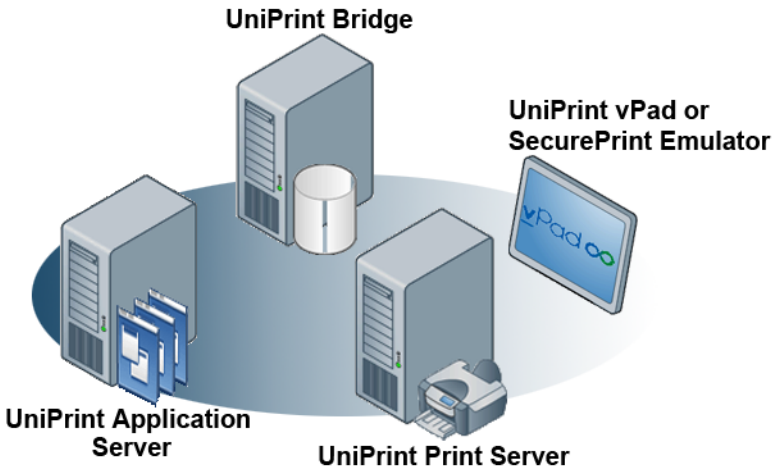
a) **OPTIONAL**: If print job statistics is being deployed, install the **Statistics Client** on the same server machine as UniPrint Application Server. Also install the **Statistics Server** on a separate, independent server machine that has the same recommended system requirements as the UniPrint Bridge.

3. Install **UniPrint Client** on a workstation with an accessible hard drive. Refer to the UniPrint Client Administrator's Guide included in the UniPrint Client download package for information on installing and configuring the UniPrint Client.

After installing all components and options, the UniPrint Infinity Client/Server environment may look similar to the following diagram.



Print Server Scenario



In this scenario, workstation and/or thin-client users print from RDP and/or ICA sessions to network printers. Three components are required to be installed on three servers -- UniPrint Bridge with the License Server, UniPrint Print Server and UniPrint Application Server. UniPrint Client is optional and is only required for those printing to client-attached desktop printers. This environment also allows for SecurePrint, PrintPAL, and mobile printing solutions, such as, UniPrint Mobile Printing, AirPrint Printing Module and Email2Print to be deployed.

The recommended installation order for a Print Server deployment is as follows:

1. Install **UniPrint Bridge** on a server. ***Note**: The **UniPrint License Server** component is packaged with the UniPrint Bridge installation file. The UniPrint License Server does not necessarily have to be installed on the same server as the UniPrint Bridge, but only one instance of the UniPrint License Server can exist in your UniPrint Infinity deployment.*

    a) For secure pull printing, Print Delegation, and Print Stream Compression, install the **SecurePrint Server** component on the UniPrint Bridge.

    b) PrintPAL is used to automatically map printers to user sessions and the **PrintPAL Server** component is installed on the UniPrint Bridge by default.

2. Install **UniPrint Print Server** on network print servers. ***Note**: It is NOT recommended to have the UniPrint Bridge and the UniPrint Print Server running on the same server machine.*

    a) For secure pull printing, Print Delegation and Print Stream Compression, install the **SecurePrint print server components** on the same machine as the UniPrint Print Server. The vPad device or SecurePrint Emulator needs to connect to this print server in order to release print jobs to the appropriate printer.

    b) **OPTIONAL**: If print job archiving is being deployed, install the **Archive Client** on the same server machine as the UniPrint Print Server and also install the **Archive Server** on a separate, independent file storage server or device.

    c) **OPTIONAL**: If print job statistics is being deployed, install the **Statistics Client** on the same server machine as the UniPrint Print Server. Also install the **Statistics Server** on a separate, independent server machine that has the same recommended system requirements as the UniPrint Bridge.

3. Install **UniPrint Application Server** on a Remote Desktop/Citrix server. If Adobe Reader or Acrobat are already installed, the **Adobe**

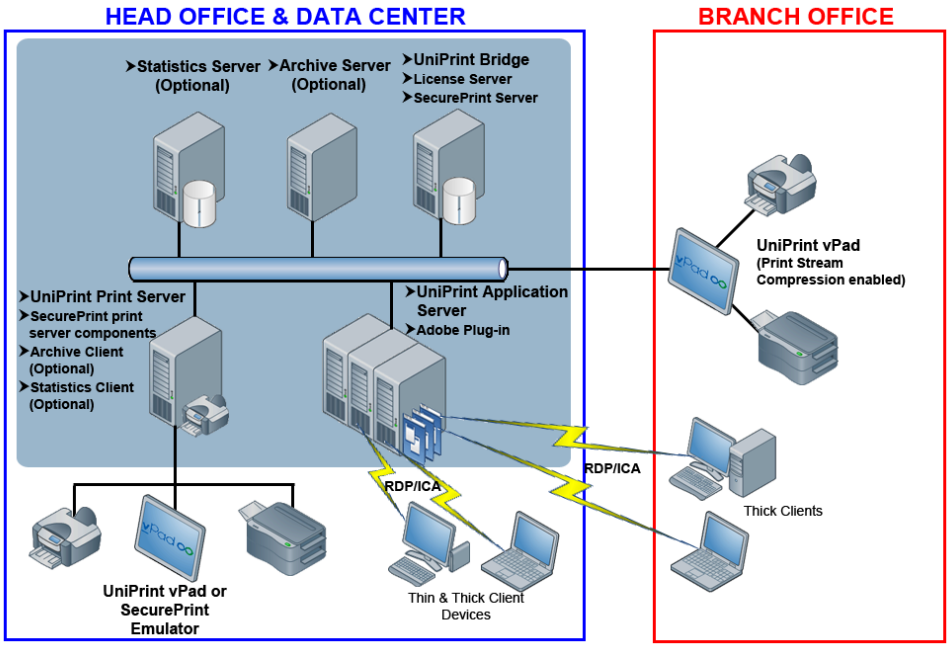
Plug-in is installed by default for users who print documents that are already in PDF format.

NOTE: It is **HIGHLY RECOMMENDED** that the Adobe Plug-in be installed since it prevents UniPrint from re-rendering PDFs. Re-rendered PDFs often results in replaced or missing fonts and sometimes the re-rendered PDF size can be much larger than the original file size if the Adobe Plug-in is not used. The Adobe Plug-in should always be installed unless it is known for sure that users will not be printing PDFs from Adobe Reader or Acrobat.

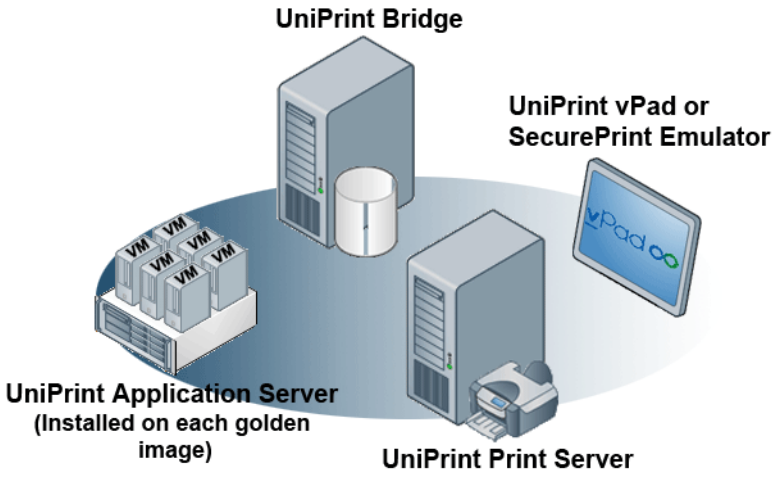
NOTE: To reduce printing downtime, it is recommended that the UniPrint Bridges and/or the UniPrint Print Servers be set up in a High Availability (HA) setup. For information on deploying UniPrint Infinity in an HA environment, refer to the UniPrint Infinity High Availability Setup Guide.

4. **OPTIONAL**: To enable users to print to their desktop printers from their sessions, install the UniPrint Client on the user's desktop machine.

After installing all components and options, the UniPrint Infinity Print Server environment will look similar to the following diagram.



VDI Scenario



In this environment, users print from within virtual desktop sessions. This environment can consist of various VDI endpoints, including zero clients, thin clients, desktop machines or a combination for the aforementioned endpoints. Three components are required to be installed on two servers and on all golden images - UniPrint Bridge with the License Server, UniPrint Print Server and UniPrint Application Server/Infinity Agent.

The recommended installation order for a VDI deployment is as follows:

1. Install **UniPrint Bridge** on a server. ***Note**: The **UniPrint License Server** component is packaged with the UniPrint Bridge installation file. The UniPrint License Server does not necessarily have to be installed on the same server as the UniPrint Bridge, but only one instance of the UniPrint License Server can exist in your UniPrint Infinity deployment.*

    a) For secure pull printing, Printer Delegation, and Print Stream Compression, install the **SecurePrint Server** on the UniPrint Bridge.

    b) PrintPAL is used to automatically map printers to user sessions and the **PrintPAL Server** is installed by default on the UniPrint Bridge.

2. Install **UniPrint Print Server** on network print servers. ***Note**: It is NOT recommended to have the UniPrint Bridge and the UniPrint Print Server running on the same server machine.*

a) For secure pull printing, Printer Delegation, and Print Stream Compression, install the **SecurePrint print server components** on the same machine as the UniPrint Print Server. The vPad device or SecurePrint Emulator will need to connect to this print server in order to release print jobs to the appropriate printer.

b) **OPTIONAL**: If print job archiving is being deployed, install the **Archive Client** on the same server machine as the UniPrint Print Server and also install the **Archive Server** on a separate, independent, file storage machine.

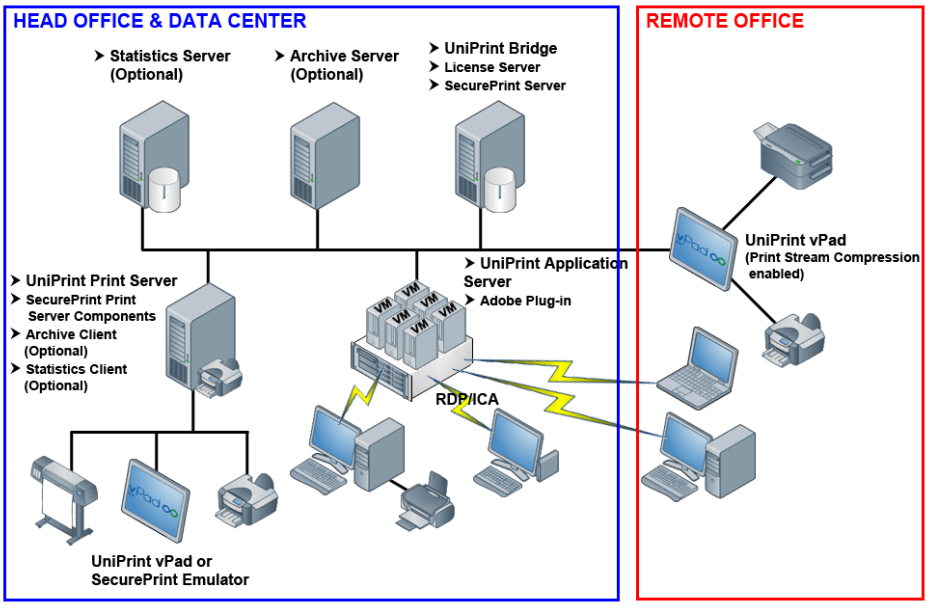
c) **OPTIONAL**: If print job statistics is being deployed, install the **Statistics Client** on the same server machine as UniPrint Print Server. Also install the **Statistics Server** on a separate, independent server machine that has the same recommended system requirements as the UniPrint Bridge.

3. Install UniPrint Application Server on all golden images or the **Infinity Agent** on existing virtual/physical desktops. The Infinity Agent Installer will install **UniPrint Application Server** without the **Management Console**. The **No static connection to the Bridge Server** option and **PrintPAL** are also enabled. This agent can be downloaded from https://www.uniprint.net/members/download/agent/InfinityAgentInstaller911.exe.

NOTE: It is **HIGHLY RECOMMENDED** that the Adobe Plug-in be installed since it prevents UniPrint from re-rendering PDFs. Re-rendered PDFs often results in replaced or missing fonts and sometimes the re-rendered PDF size can be much larger than the original file size if the Adobe Plug-in is not used. The Adobe Plug-in should always be installed unless it is known for sure that users will not be printing PDFs from Adobe Reader or Acrobat.

4. **OPTIONAL**: To enable users to print to their desktop printers from their VDI sessions, install the **UniPrint Client** on the user desktop machine.

After installing all components and options, the UniPrint Infinity VDI environment may look similar to the following diagram.



Installing UniPrint Infinity

The following instructions assume that you are installing UniPrint Infinity on Windows Server 2012 R2. If you are installing on another platform, you will need to adjust the steps to account for any interface differences. Consult the product documentation for your operating system.

Before installing UniPrint Infinity, it is recommended that you take note of the License Server (UniPrint Bridge) IP address. This information is required when installing UniPrint Print Server and UniPrint Application Server.

Non-interactive command line installation of UniPrint is available. For command line installation instructions, see "Installing UniPrint from the Command Line" on page 44.

Installing UniPrint Bridge And its Components

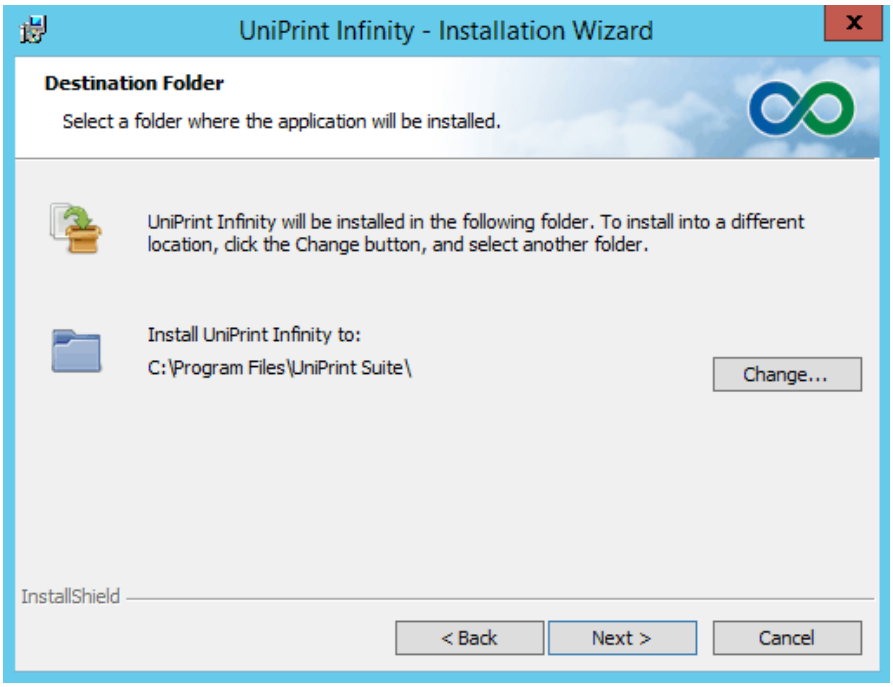
The UniPrint Bridge and its components are typically the first components to be installed in all deployment scenarios and should be installed on its own server machine.

1. On a server machine that meets the recommended system requirements, run the installation program, **UniPrint91_*.exe** as an administrator.

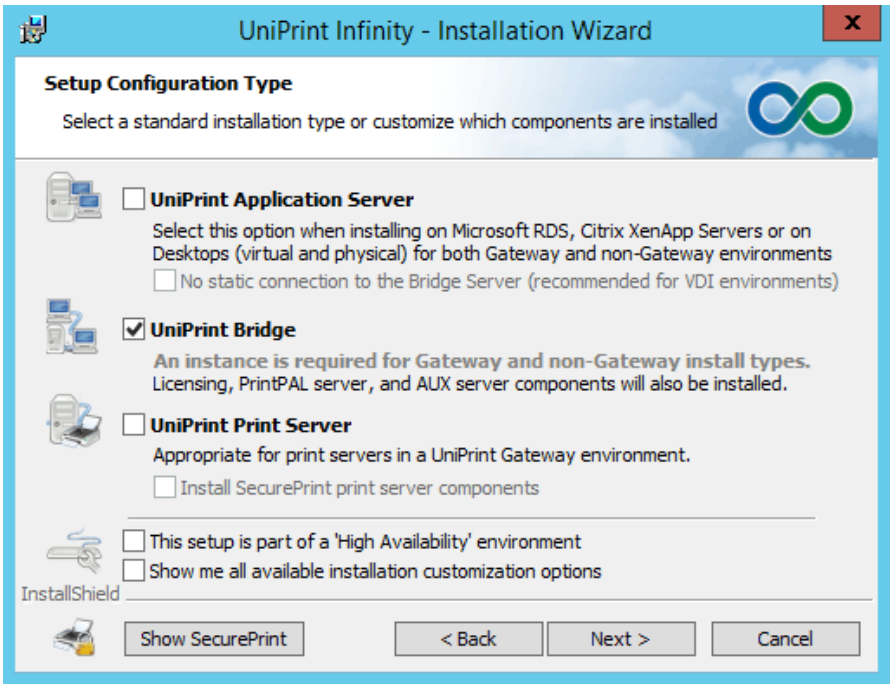
2. In the **UniPrint Infinity Installation** dialog box, click **Next**.

3. In the **License Agreement** dialog box, click **I accept the terms in the license agreement** and then click **Next**.

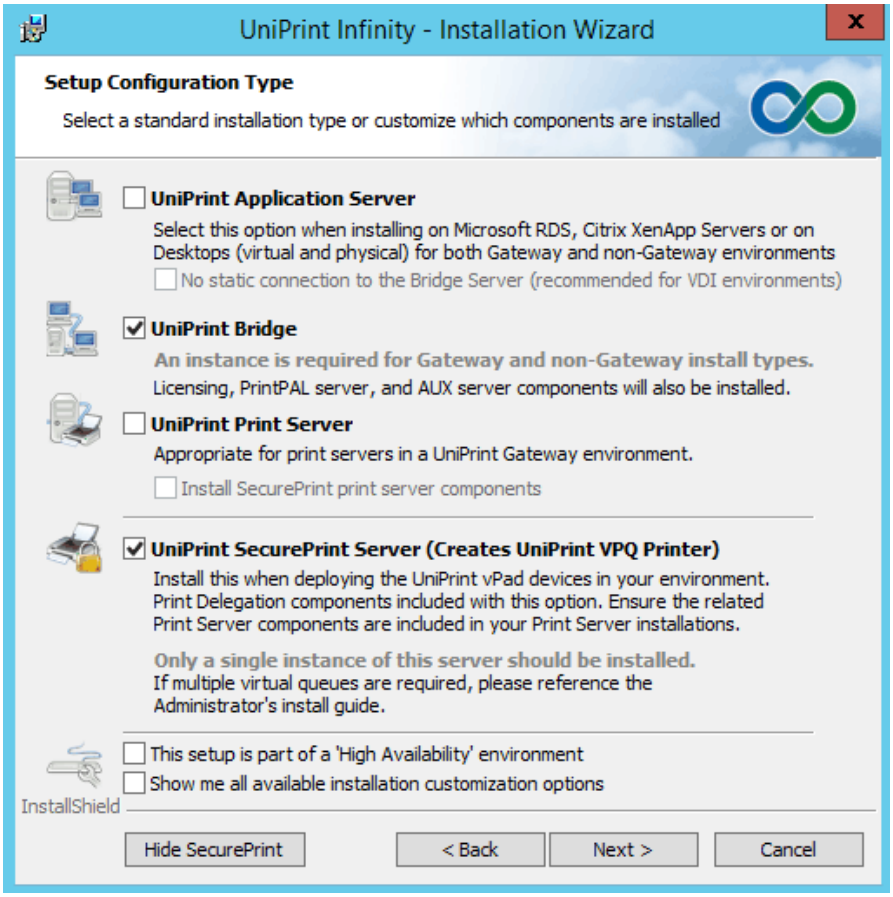
4. In the **Destination Folder** dialog box, click **Next** to accept the default location for the UniPrint program files. To select a different location, click **Change** and then browse to the alternate location.



5. In the **Setup Configuration Type** dialog box, select **UniPrint Bridge**.



a) For SecurePrint and Print Stream Compression deployments, click **Show SecurePrint**. Then select **UniPrint SecurePrint Server (Creates UniPrint VPQ Printer)**.



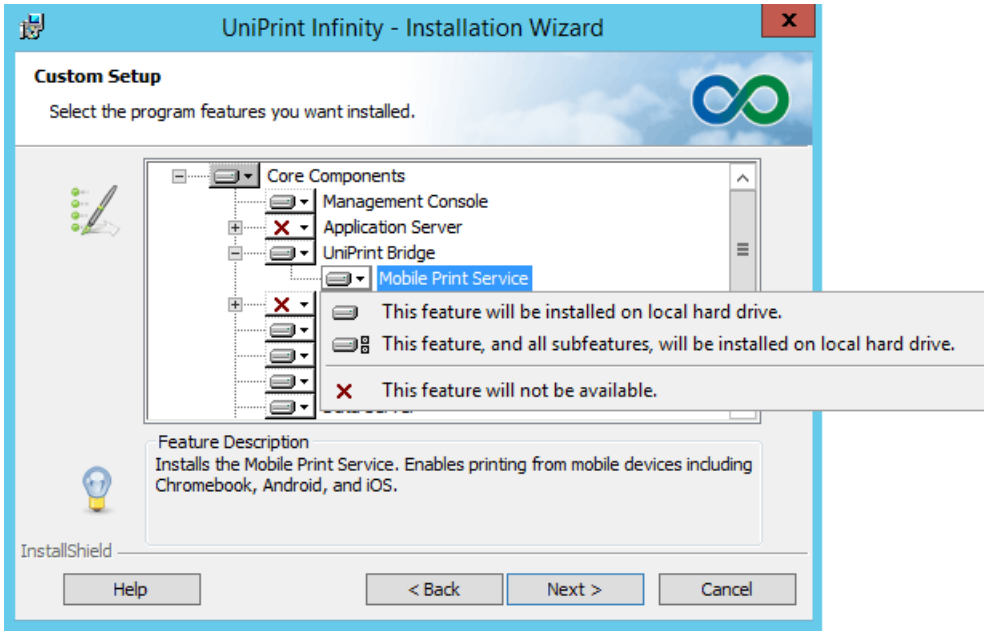
NOTE: The SecurePrint Server component must be installed even if only Print Stream Compression will be used without the UniPrint VPQ.

b) The License Server will be installed by default. If the License Server component is already installed on a different UniPrint Bridge machine, or to install additional components, select **Show me all available installation customization options.**

6. Click **Next.**

7. If **Show me all available installation customization options** was selected, the **Custom Setup** dialog box will appear. To prevent a

component from being installed, click beside the component and then select **This feature will not be available**.

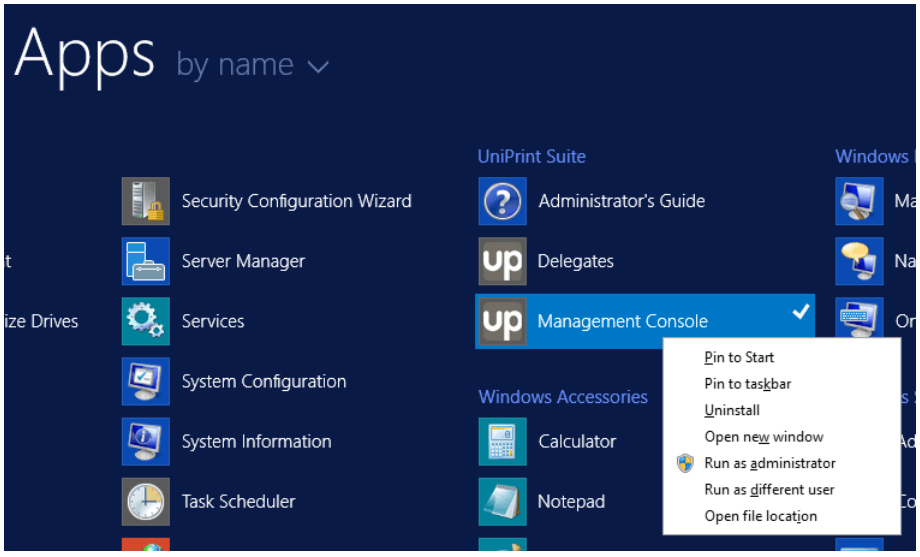


8. Click **Next**.

9. In the **Ready to Install the Program** dialog box, click **Install**. UniPrint installer will copy files to the destination folder.

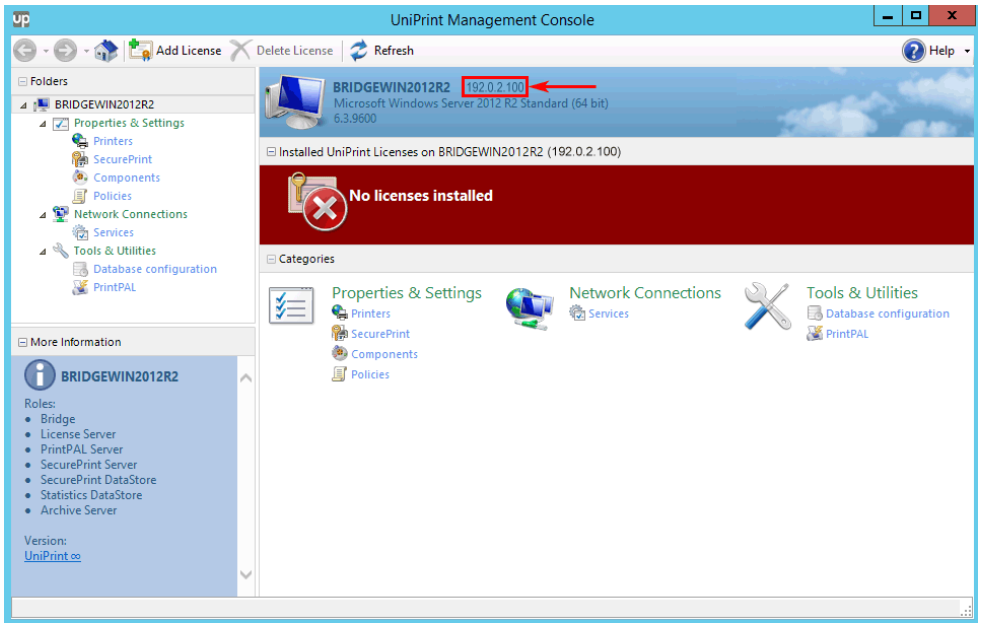
10. Click **Finish** to complete the installation.

11. Click **Start** and then under Recently added, right-click **Management Console**. Select either **Pin to Start** or point to More **Pin to taskbar** depending on how often it will be accessed.



12. Click to return to the **Start** screen and if **Pin to taskbar** was selected, click the **Desktop** tile. Click to open the **UniPrint Management Console**.

13. At the top of the console, take note of the IP address. This is required when installing the UniPrint Print Server and the UniPrint Application Server.



Installing UniPrint Print Server And its Components

The UniPrint Print Server and its components are typically the second components to be installed in Print Server and VDI environments.

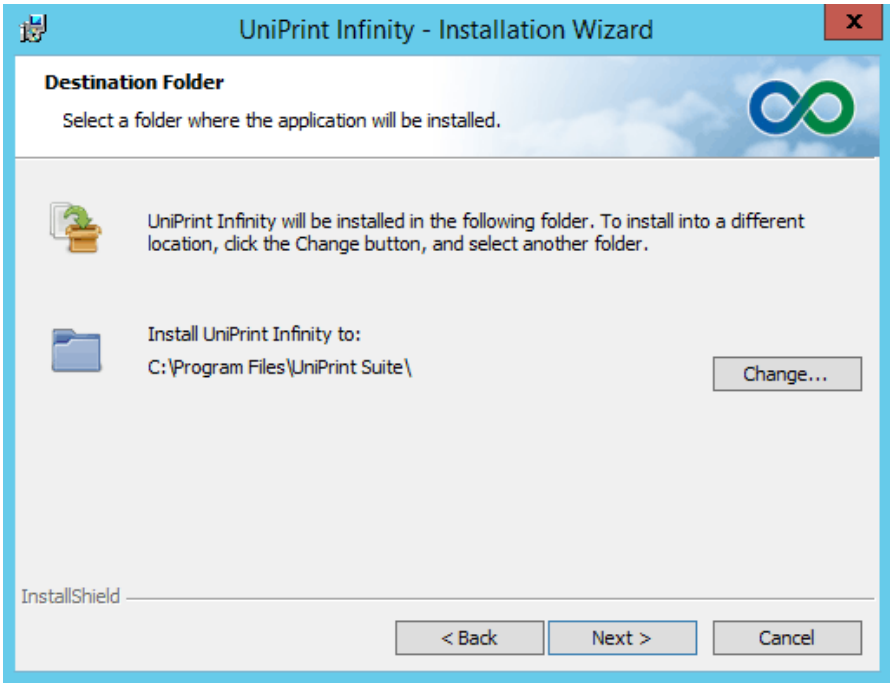
For Client/Server environments, the UniPrint Print Server component is not required. Continue the installation process by "Installing UniPrint Application Server And Its Components" on page 32.

1. On a network print server that meets the recommended system requirements, run the installation program, **UniPrint91_*.exe** as an administrator.

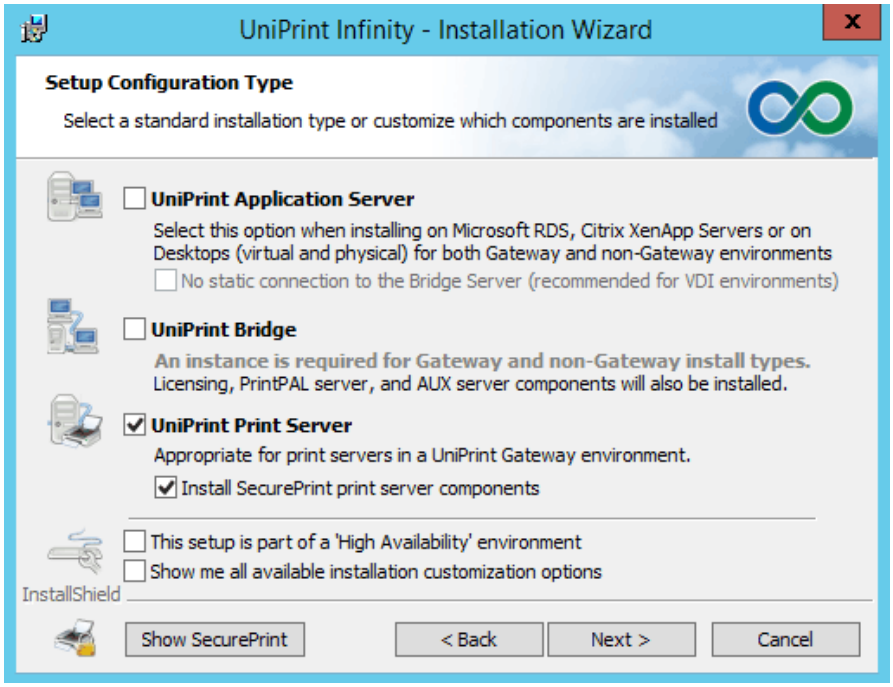
2. In the **UniPrint Infinity Installation** dialog box, click **Next**.

3. In the **License Agreement** dialog box, click **I accept the terms in the license agreement** and then click **Next**.

4. In the **Destination Folder** dialog box, click **Next** to accept the default location for the UniPrint program files. To select a different location, click **Change** and then browse to the alternate location.



5. In the **Setup Configuration Type** dialog box, select **UniPrint Print Server**.



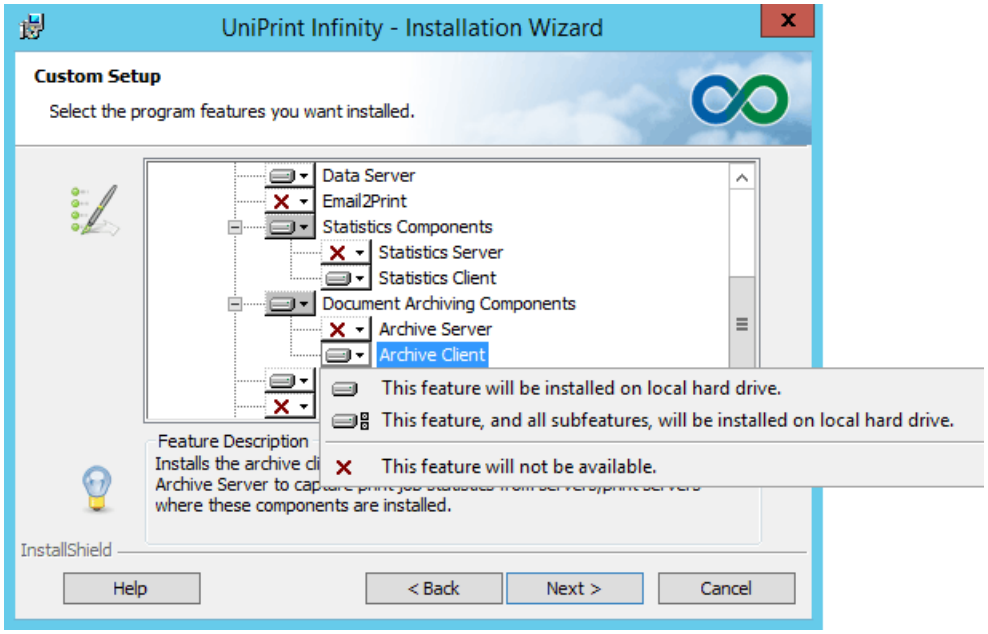
a) If secure pull printing, Printer Delegation, and Print Stream Compression, are being deployed, click **Install SecurePrint print server components.**

b) If print job archiving and/or print job statistics monitoring are being deployed, select **Show me all available installation customization options**.

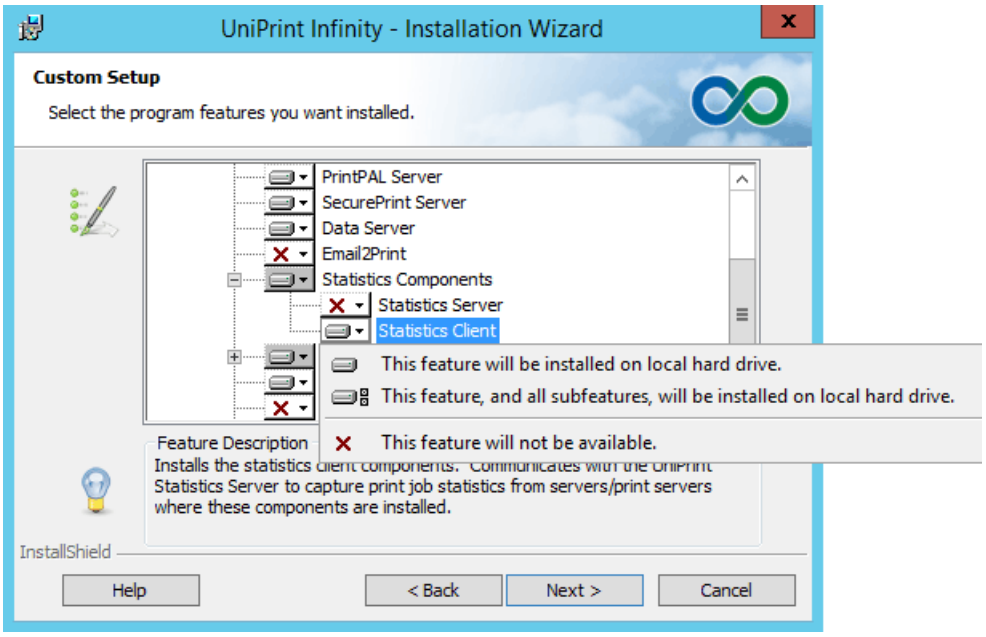
6. Click **Next.**

7. If **Show me all available installation customization** options was selected the **Custom Setup** dialog box will appear.

a) To archive print jobs directed to printers on this print server, expand **Document Archive Components**. Beside **Archive Client**, click and then select **This feature will be installed on local hard drive**.

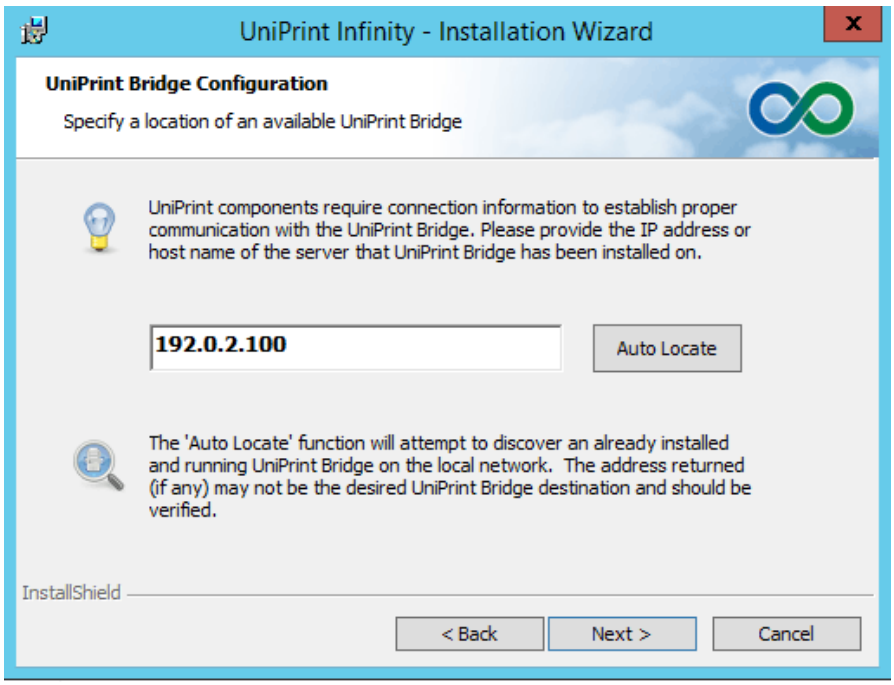


b) To monitor print job statistics for all print jobs directed to this print server, expand **Statistics Components.** Beside **Statistics Client**, click and then select **This feature will be installed on local hard drive**.

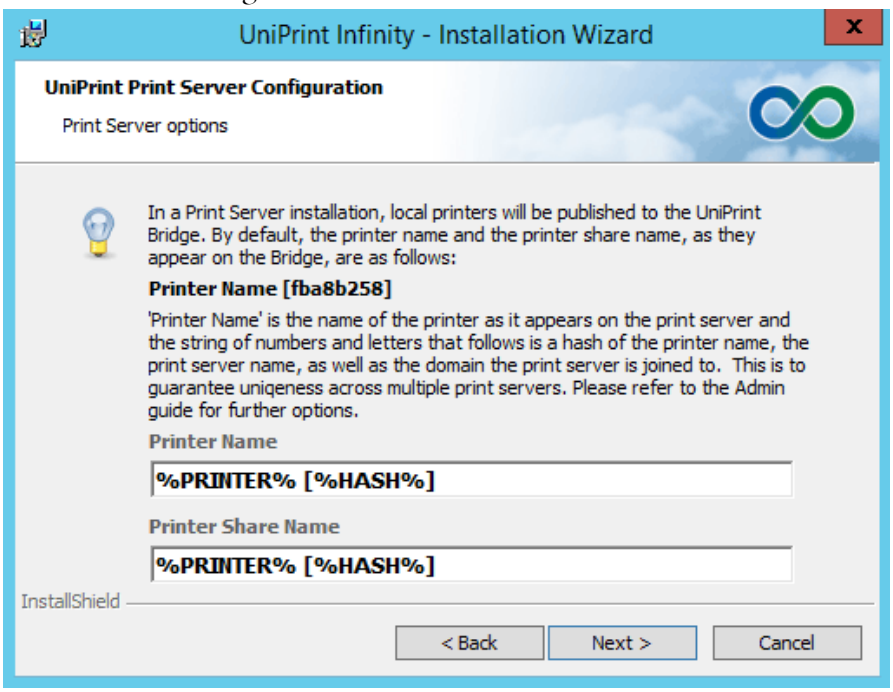


8. Click **Next**.

9. In the **UniPrint Bridge Configuration** dialog box, enter the **IP Address** of the License Server (typically the UniPrint Bridge) or click **Auto Locate** to run an auto-discovery function to find an already installed and running License Server. ***NOTE****: If using the* ***Auto Locate*** *function in an environment where there are multiple UniPrint Bridges, ensure that the discovered IP address is that of the intended License Server before proceeding*. Click **Next** to continue.



10. In the **UniPrint Print Server Configuration** dialog box, change how printers are published to the Bridge. It is recommended that the hash number not be changed since it ensures printer uniqueness across print servers. This setting can be changed after installation in the UniPrint Management Console. Click **Next**.



11. In the **Ready to Install the Program** dialog box, click **Install**. UniPrint installer will copy files to the destination folder.

12. Click **Finish** to complete the installation.

Installing UniPrint Application Server And Its Components

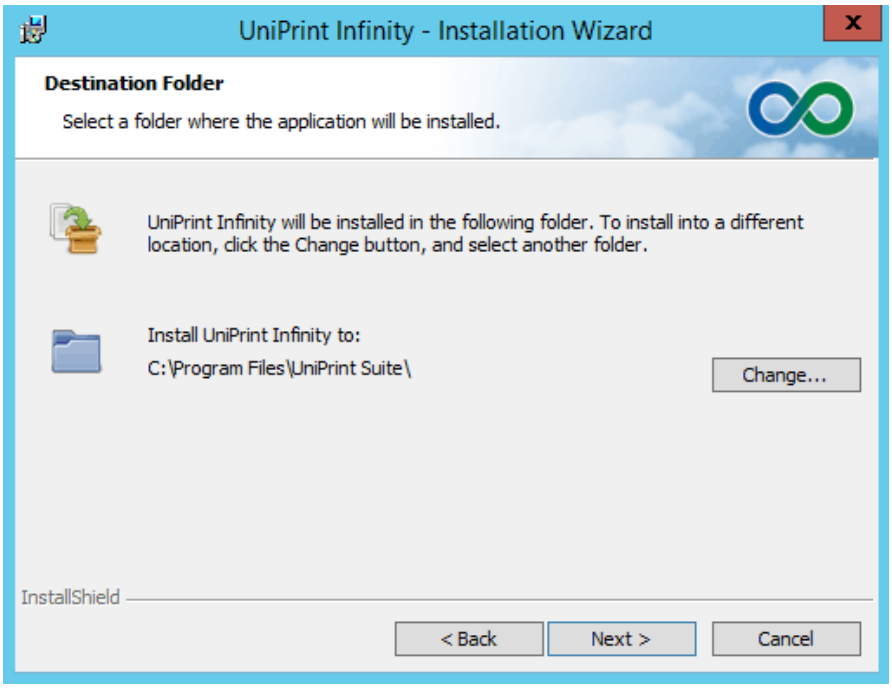
The UniPrint Application Server and its components are the second components to install in a Client/Server environment and the third components to install in a Print Server and VDI environment. For large VDI environments, it is recommended that the Infinity Agent be installed instead. The Infinity Agent is a pre-configured version of the UniPrint Application Server. However, if manual configuration is desired, then the UniPrint Application Server can be installed on a golden image using these instructions along with the recommended configuration suggestions. For detailed instructions on installing the Infinity Agent, see "Installing the Infinity Agent for VDI Environments" on page 38.

1. On a Citrix/RDS server or golden virtual desktop image that meets the recommended system requirements, run the installation program, **UniPrint91_*.exe** as an administrator.

2. In the **UniPrint Infinity Installation** dialog box, click **Next**.

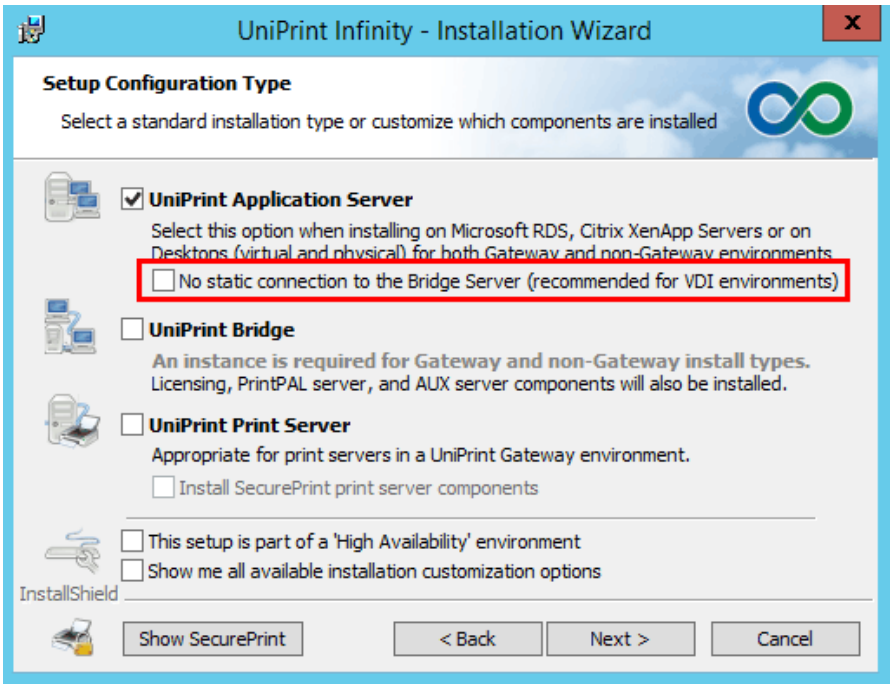
3. In the **License Agreement** dialog box, click **I accept the terms in the license agreement** and then click **Next**.

4. In the **Destination Folder** dialog box, click **Next** to accept the default location for the UniPrint program files. To select a different location, click **Change** and then browse to the alternate location.



5. In the **Setup Configuration Type** dialog box, select **UniPrint Application Server.** For VDI environments, also select **No static connection to the Bridge Server (recommended for VDI environments)**. This option instructs UniPrint to establish a

connection between the Application Server and the Bridge only when the user prints.



NOTE: If you plan on using font replication, such that font embedding is no longer necessary, then DO NOT enable the **No static connection to the Bridge Server** option. Font replication will not function properly if this option is enabled.

a) If Adobe Reader or Acrobat are already installed, then by default the Adobe Plug-in is also installed.

NOTE: It is **HIGHLY RECOMMENDED** that the Adobe Plug-in be installed since it prevents UniPrint from re-rendering PDFs. Re-rendered PDFs often results in replaced or missing fonts and sometimes the re-rendered PDF size can be much larger than the original file size if the Adobe Plug-in is not used. The Adobe Plug-in should always be installed unless it is known for sure that users will not be printing PDFs from Adobe Reader or Acrobat.

To prevent the Adobe Plug-in from being installed or to install additional components, select **Show me all available installation customization options**.

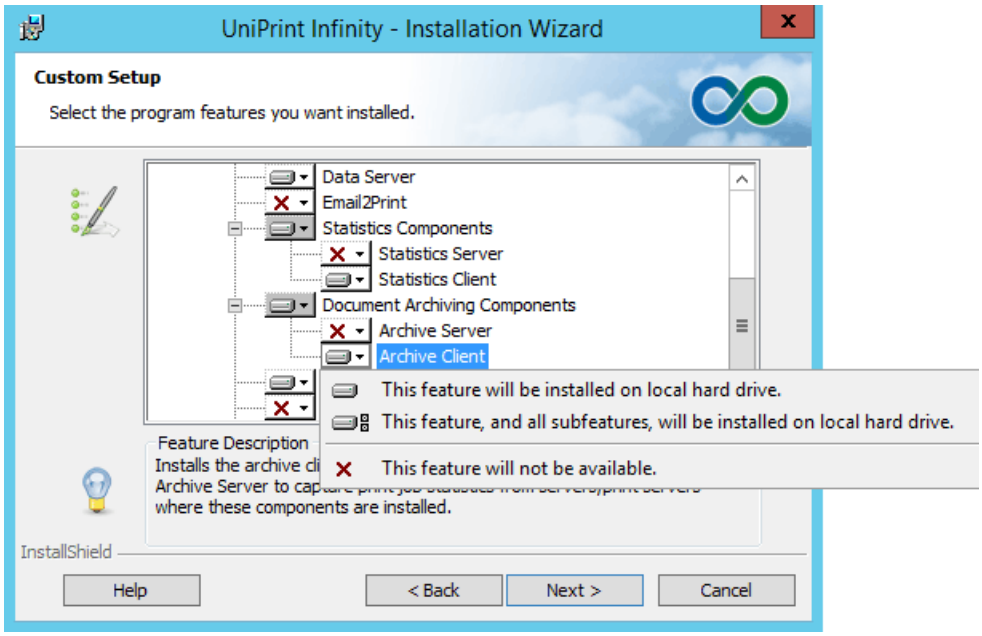
b) If print job archiving and/or print job statistics monitoring on the UniPrint or the UniPrint (Email PDF) queues are being deployed, select **Show me all available installation customization options.**

6. Click **Next.**

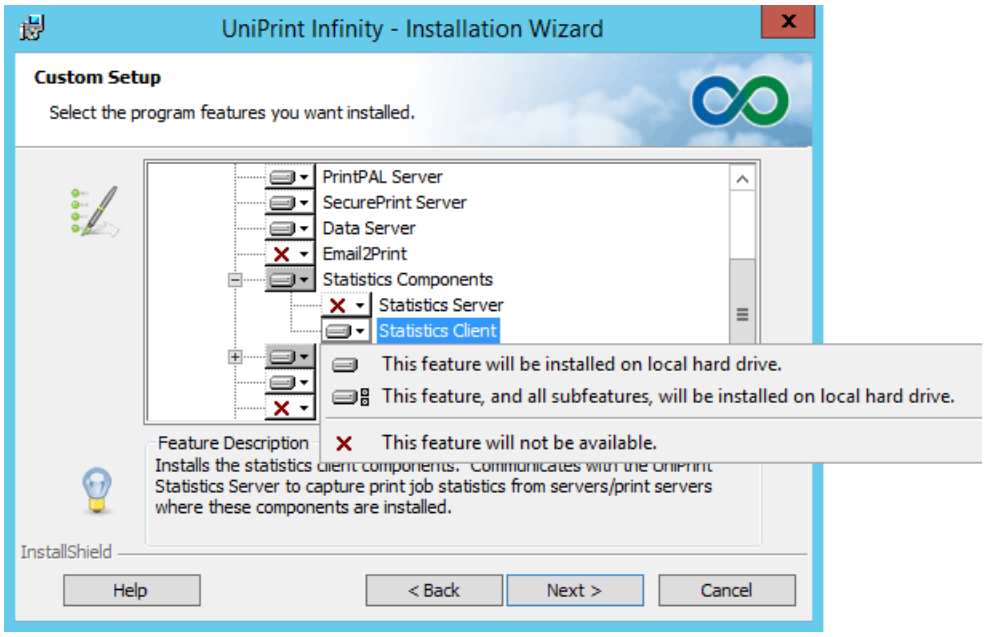
7. If **Show me all available installation customization options** was selected, the **Custom Setup** dialog box will appear.

   a) To disable a component, click beside the component and then select **This feature will not be available**.

   b) To archive print jobs sent the UniPrint queue and/or the UniPrint (Email PDF) queue, expand **Document Archiving Components** and then select **This feature will be installed on local hard drive**.

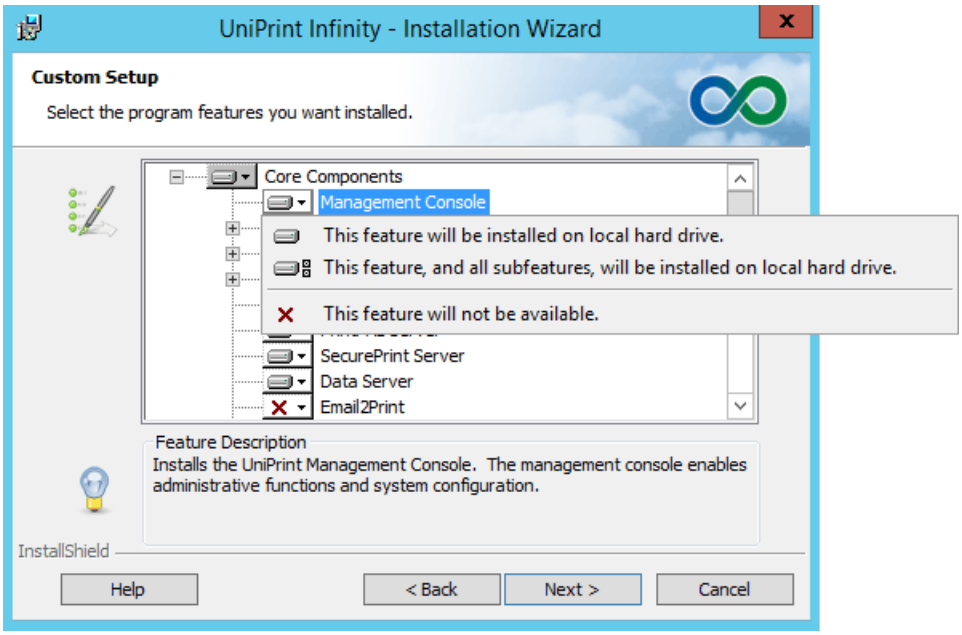


   c) To capture print job statistics for print jobs sent to the UniPrint queue, the UniPrint (Email PDF) and UniPrint (Save PDF) queues, expand **Statistics Components** and then select **This feature will be installed on local hard drive**.



d) In a VDI environment, it is recommended that the **Management Console** not be installed on the golden virtual desktop image.

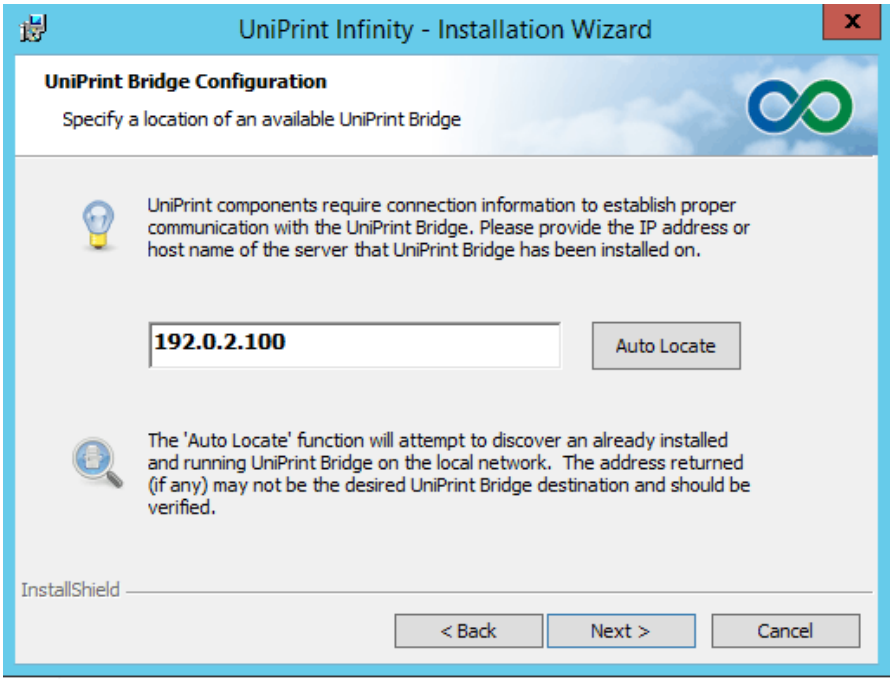
Beside **Management Console**, click and then select **This feature will not be available**.



8. Click **Next**.

9. In the **UniPrint Bridge Configuration** dialog box, enter the **IP Address** of the License Server (typically the UniPrint Bridge) or click **Auto Locate** to run an auto-discovery function to find an already installed and running License Server. ***NOTE**: If using the **Auto Locate***

function in an environment where there are multiple UniPrint Bridges, ensure that the discovered IP address is that of the intended License Server before proceeding. Click **Next** to continue.



10. In the **Ready to Install the Program** dialog box, click **Install**. UniPrint installer will copy files to the destination folder.

11. Click **Finish** to complete the installation.

12. For Client/Server environments, proceed by installing the UniPrint Client on all desktop machines accessing the Citrix/RDS server through ICA or RDP. This is optional for Print Server and VDI environments. UniPrint Client is a separate download package and can be downloaded from www.uniprint.net/eng/products/view/uniprint-client. Follow the instructions for installing UniPrint Client that are included with the download package.

13. For print job archiving, proceed by installing the Archive Server on a server machine that meets the same system requirements as the UniPrint Bridge. Refer to "Installing the Infinity Agent for VDI Environments" on page 38.

14. For print job statistics monitoring, proceed by installing the Statistics Server on a server machine that meets the same system requirements as the UniPrint Bridge. Refer to "Installing the Statistics Server Component" on page 42.

Installing the Infinity Agent for VDI Environments

For VDI environments, especially large deployments, it is recommended that the Infinity Agent be installed instead of installing UniPrint Application Server manually. The Infinity Agent installs the UniPrint Application Server along with recommended configuration settings for VDI environments. The Infinity Agent Installer can be downloaded from https://www.uniprint.net/members/download/agent/InfinityAgentInstaller911.exe.

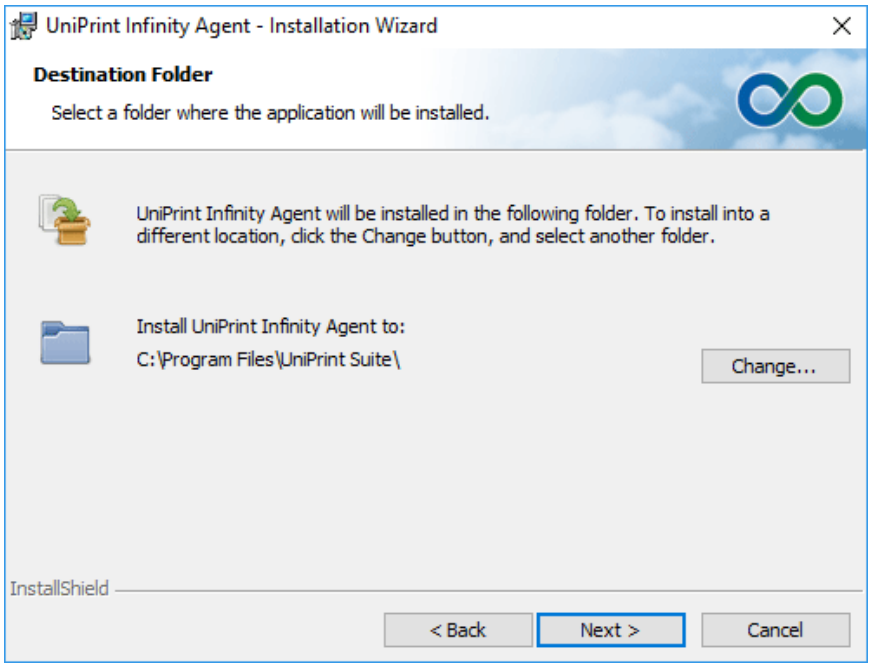
To install the Infinity Agent on each virtual desktop golden image, do the following:

1. Run the **Infinity Agent Installer** by double-clicking **InfinityAgentInstaller911.exe**. If **User Access Control** appears, click **Yes** to continue.

2. In the **UniPrint Infinity Agent Installation** dialog box, click **Next**.

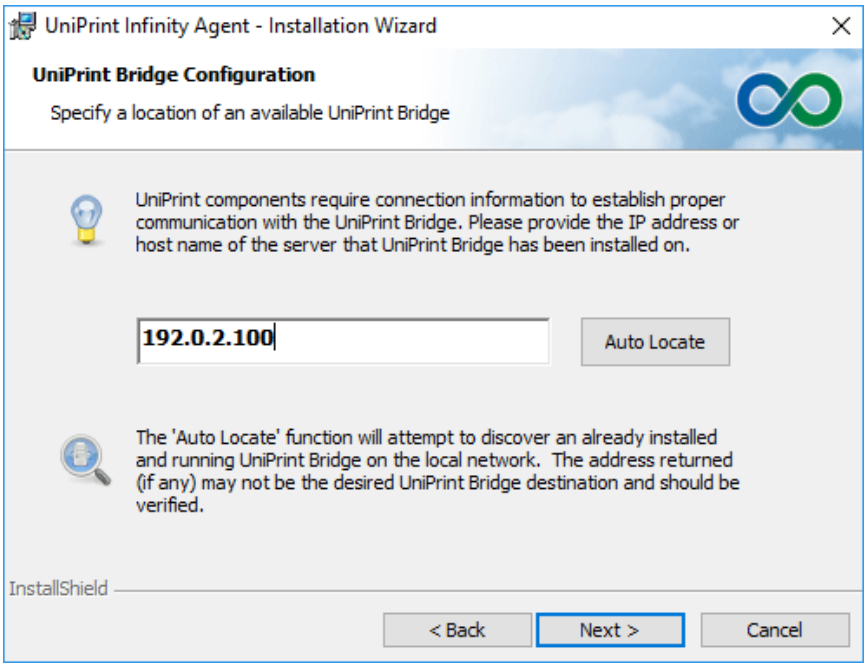
3. In the **License Agreement** dialog box, click **I accept the terms in the license agreement** and then click **Next**.

4. In the **Destination Folder** dialog box, click **Next** to accept the default location for the UniPrint program files. To select a different location, click **Change** and then browse to the alternate location.



5. In the **UniPrint Bridge Configuration** dialog box, enter the **IP Address** of the License Server (typically the UniPrint Bridge) or click **Auto Locate** to run an auto-discovery function to find an already

installed and running License Server. ***NOTE**: If using the **Auto Locate** function in an environment where there are multiple UniPrint Bridges, ensure that the discovered IP address is that of the intended License Server before proceeding.* Click **Next** to continue.



6. In the **Ready to Install the Program** dialog box, click **Install**. UniPrint installer will copy files to the destination folder.

7. Click **Finish** to complete the installation.

Installing the Archive Server Component

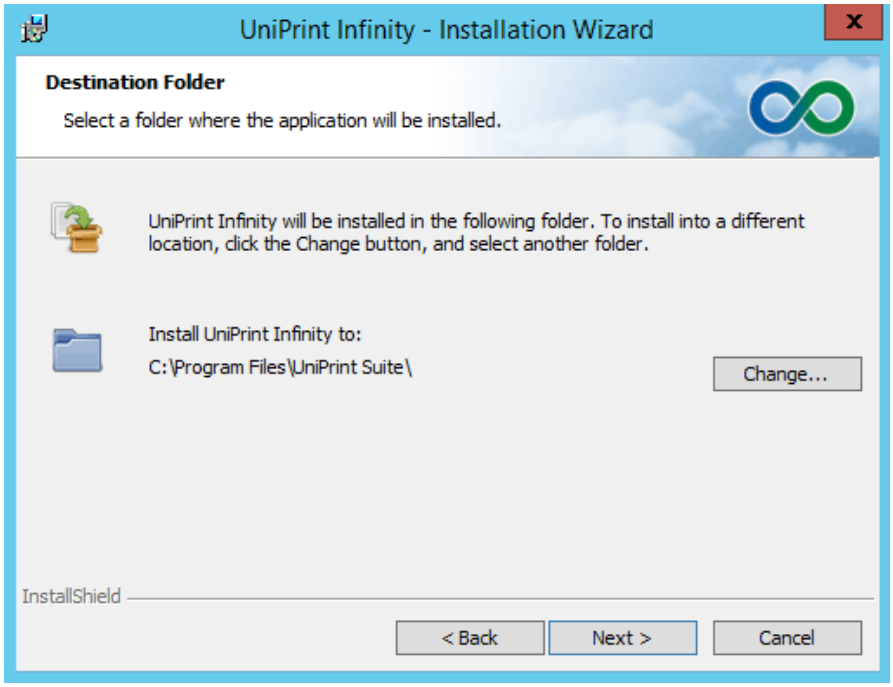
The Archive Server component is installed on the file storage server that will host archived print jobs. This component must meet the same recommended system requirements as the UniPrint Bridge and the storage capacity required depends on the amount of printing done within an organization.

1. On the intended archive server, right-click the installation program, **UniPrint91_*.exe** and select **Run as administrator**.

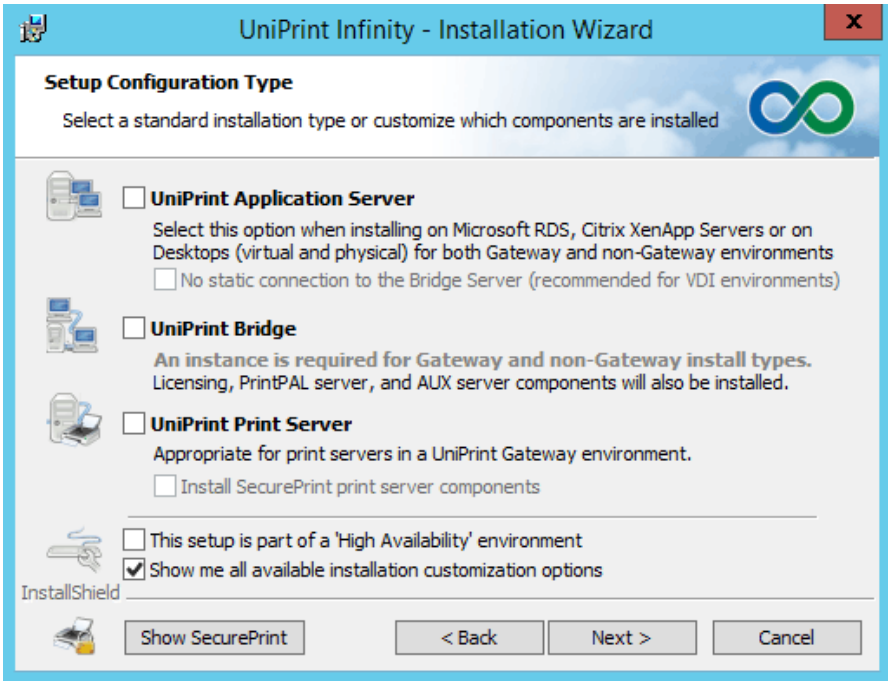
2. In the **UniPrint Infinity Installation** dialog box, click **Next**.

3. In the **License Agreement** dialog box, click **I accept the terms in the license agreement** and then click **Next**.

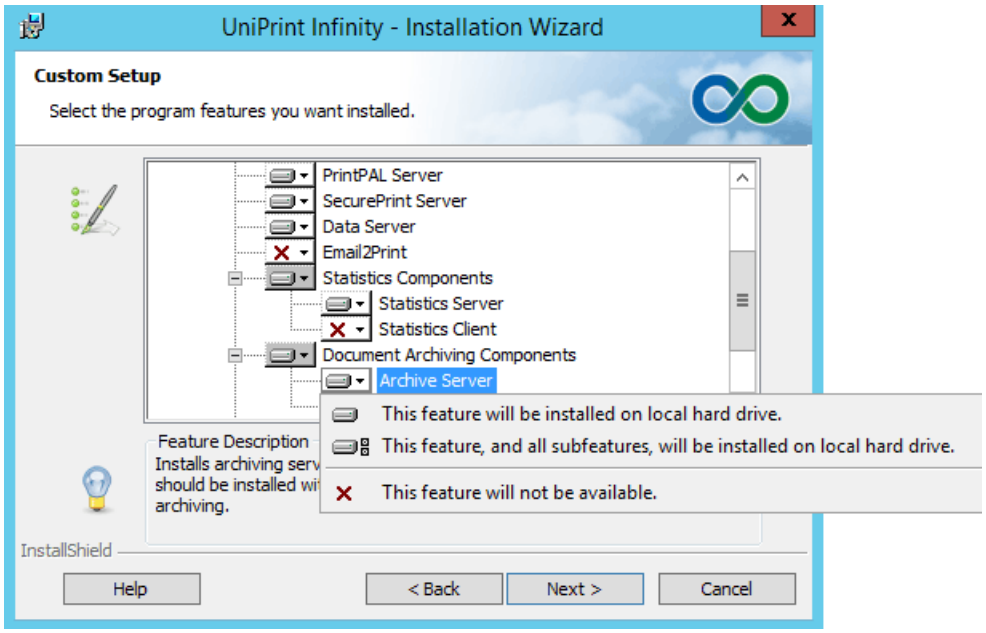
4. In the **Destination Folder** dialog box, click **Next** to accept the default location for the UniPrint program files. To select a different location, click **Change** and then browse to the alternate location.



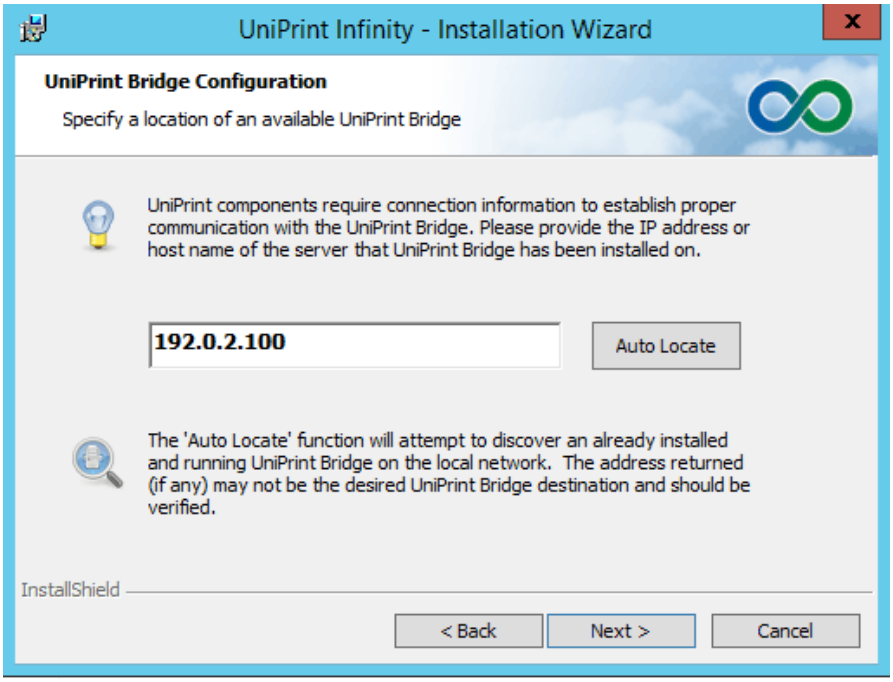
5. In the **Setup Configuration Type** dialog box, select **Show me all available installation customization options** and then click **Next**.



6. In the **Custom Setup** dialog box, expand **Document Archiving Components**. Beside **Archive Server**, click and then select



7. In the **UniPrint Bridge Configuration** dialog box, enter the **IP Address** of the License Server (typically the UniPrint Bridge) or click **Auto Locate** to run an auto-discovery function to find an already installed and running License Server. ***NOTE****: If using the* ***Auto Locate*** *function in an environment where there are multiple UniPrint Bridges, ensure that the discovered IP address is that of the intended License Server before proceeding.* Click **Next** to continue.



8. In the **Ready to Install the Program** dialog box, click **Install**. UniPrint installer will copy files to the destination folder.

9. Click **Finish** to complete the installation.

Installing the Statistics Server Component

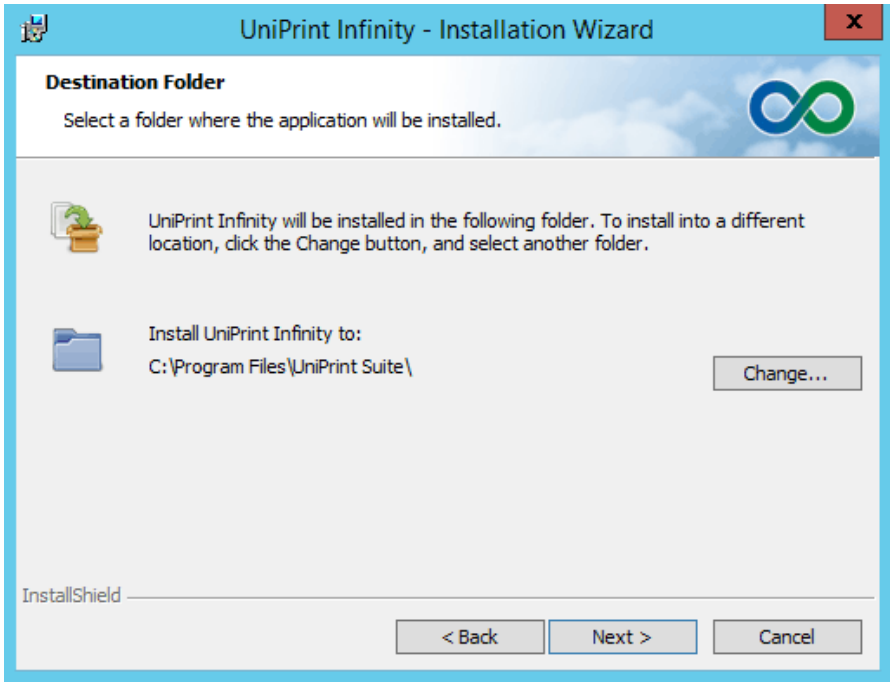
The Statistics Server component is installed on a server machine that has the same system requirements as the UniPrint Bridge. This server will host all captured print job data in a database.

1. On the intended statistics server, run the installation program, **UniPrint91_*.exe** as an administrator.

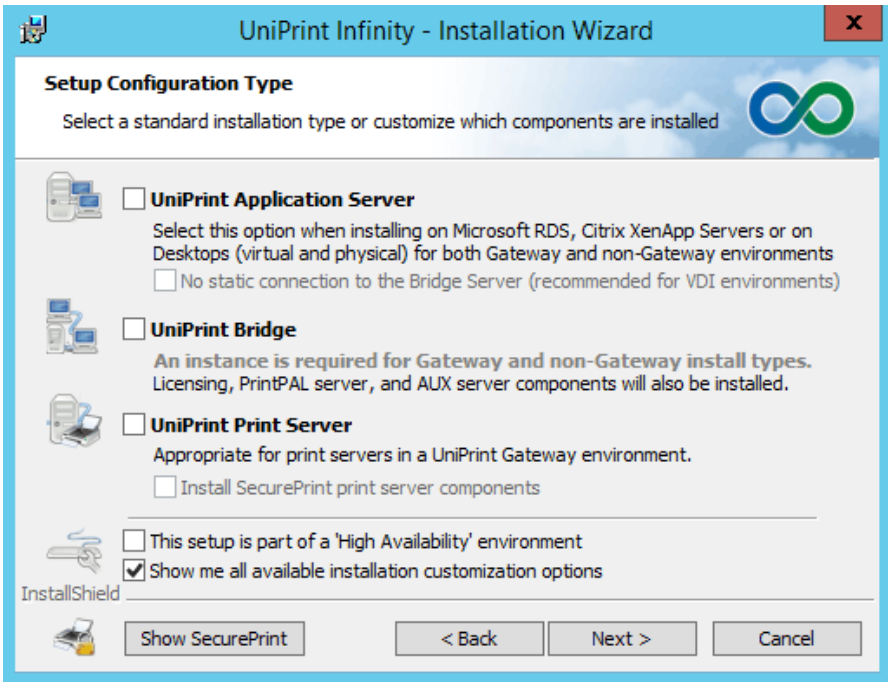
2. In the **UniPrint Infinity Installation** dialog box, click **Next**.

3. In the **License Agreement** dialog box, click **I accept the terms in the license agreement** and then click **Next**.

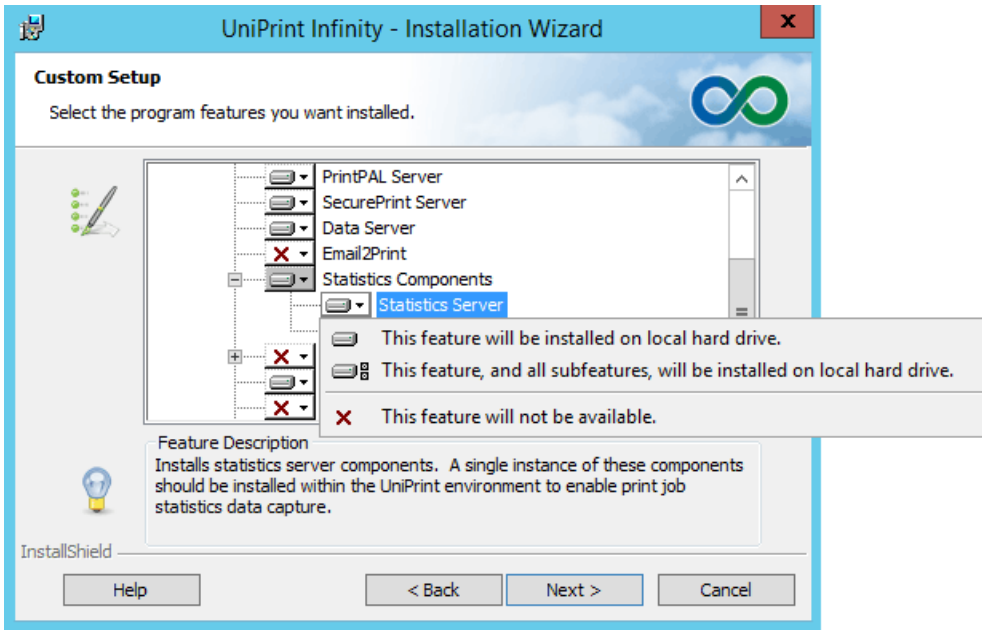
4. In the **Destination Folder** dialog box, click **Next** to accept the default location for the UniPrint program files. To select a different location, click **Change** and then browse to the alternate location.



5. In the **Setup Configuration Type** dialog box, select **Show me all available installation customization options** and then click **Next**.

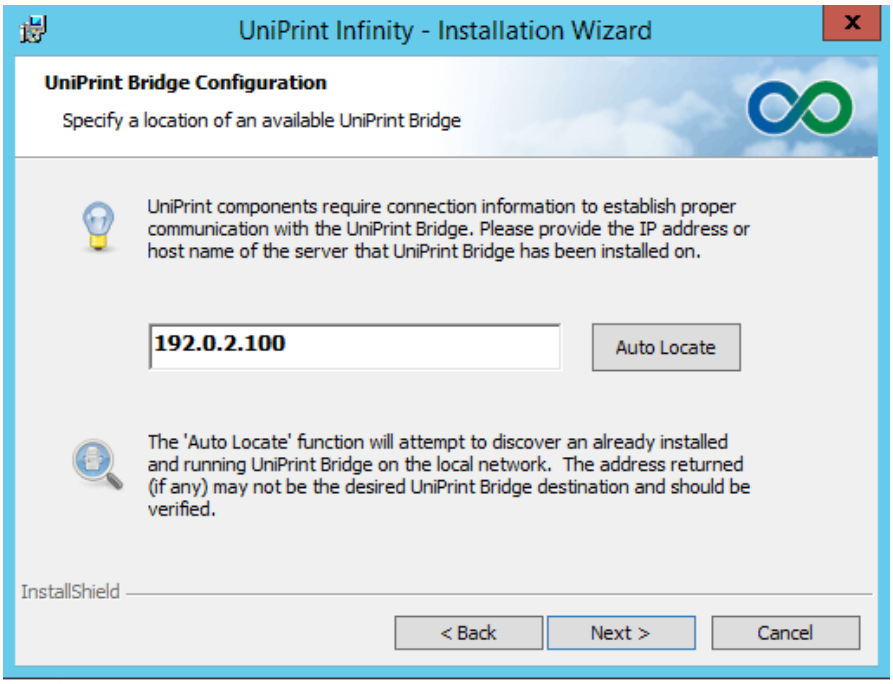


6. In the **Custom Setup** dialog box, expand **Statistics Components**. Beside **Statistics Server,** click and then select **This feature will be installed on local hard drive.**



7. In the **UniPrint Bridge Configuration** dialog box, enter the **IP Address** of the License Server (typically the UniPrint Bridge) or click **Auto Locate** to run an auto-discovery function to find an already

installed and running License Server. ***NOTE**: If using the **Auto Locate** function in an environment where there are multiple UniPrint Bridges, ensure that the discovered IP address is that of the intended License Server before proceeding.* Click **Next** to continue.



8. In the **Ready to Install the Program** dialog box, click **Install**. UniPrint installer will copy files to the destination folder.

9. Click **Finish** to complete the installation.

Installing UniPrint from the Command Line

Command line installation is available for UniPrint91_*.msi with the following options. A restart is required after command line installation.

NOTE: If UAC is enabled, msiexec.exe must be run as an administrator. To run a command line as an administrator do the following:
1. Click **Start** and then click .
2. Under **Windows System**, right-click **Command Prompt** and then select **Run as administrator.**

Syntax

UniPrint Bridge **msiexec /q /i c:\UniPrint91_*.msi ADDLOCAL=Bridge,[Administrative_Console],[License_Server],**

[**SecurePrint_Server**],[**AUX_Server**],[**Data_Server**],[**Email2Print**], [**Document_Conversion_Server**],[**Imprivata_Gateway**], [**Mobile_Print_Service**], [**Print_Route**] [**INSTALLDIR** = "*path*"]

UniPrint Print Server

msiexec /q /i C:\UniPrint91_*.msi ADDLOCAL=Print_Server, [**Administrative_Console**],[**SecurePrint_Components**], [**Archive_Client**],[**Statistics_Client**],[**IPPServer**] [**INSTALLDIR** = "*path*"] [**UP_SETTING_BRIDGEIP**=*nnn.nnn.nnn.nnn*:*ppppp*, *nnn.nnn.nnn.nnn:ppppp*] [**UP_SETTING_STAT_CLIENT_PORT**=*ppppp*]

UniPrint Application Server

msiexec /q /i C:\UniPrint91_*.msi ADDLOCAL=App_Server,[**Administrative_Console**], [**Adobe_Plugin**],[**Archive_Client**],[**Statistics_Client**] [**INSTALLDIR**= "*path*"] [**DOTNETVERSION40CLIENT**={**0**|**1**}] [**UP_SETTING_RUN_PRINTPAL**=#{**0**|**1**}] [**UP_SETTING_BRIDGEIP**=*nnn.nnn.nnn.nnn*:*ppppp*, *nnn.nnn.nnn.nnn:ppppp*] [**UP_SETTING_PAPERSIZE**=#*n*] [**UP_SETTING_UNIPRINT_AS_DEFAULT**=#{**0**|**1**}] [**UP_SETTING_GPO**={**M**|**U**|**S**|**D**}] [**UP_SETTING_LOGLEVEL**=*n*] [**UP_SETTING_PASSTHROUGH**=#*n*] [**UP_SETTING_NO_UNIPRINT_PRINTER**=#{**0**|**1**}] [**UP_SETTING_NO_SAVE_QUEUE**=#{**0**|**1**}] [**UP_SETTING_STAT_CLIENT_PORT**=#*ppppp*] [**UP_SETTING_VC_ORDER**={**t**|**c**|**d**|**p**|**m**}] [**USE_VDI_SERVER_SETTINGS**={**0**|**1**}]

Archive Server

msiexec /q /i C:\UniPrint91_*.msi ADDLOCAL=Archive_Server, [Administrative_Console] [INSTALLDIR="*path*"]

Statistics Server

msiexec /q /i C:\UniPrint91_*.msi ADDLOCAL=Statistics_Server, [Administrator_Console] [INSTALLDIR="*path*"] [**UP_SETTING_STAT_SERVICE_PORT**=#*ppppp*]

NOTE: A comma (,) is required between each ADDLOCAL component and a space is required between each setting. Also note that some, but not all, parameters require the number sign (#) before the parameter value.

Command Line Options

/q

Function: Runs the Setup in silent mode (no user intervention required).
Remarks: Must be used with the /i Windows Installer parameter. If no additional parameters are passed, default values will be used.
Example: `msiexec /q /i C:\UniPrint91_*.msi ADDLOCAL=Bridge`

ADDLOCAL= component

Function: Specifies which UniPrint Infinity component to install on the local server.
Remarks: Separate multiple components with a comma only and each component is case sensitive. If no additional parameters are passed, default values will be used.

Component	Description
Administrative_Console	Installs the UniPrint Management Console. By default when installing UniPrint Infinity from the command line, the Management Console is disabled.
Bridge	Installs the UniPrint Bridge components and is responsible for communication routing with the UniPrint Infinity environment.
License_Server	Installs licensing components on the UniPrint Bridge for licensing distribution to connected UniPrint Infinity servers. An instance of this component must exist within the UniPrint Infinity environment.
PrintPAL_Server	Installs the PrintPAL Server on the UniPrint Bridge for automated printer to user session mapping.
SecurePrint_Server	Installs the SecurePrint Server components on the UniPrint Bridge including the virtual print queue (VPQ). This also includes components for Printer Delegation and Print Stream Compression.
Data_Server	Install the Data Server components on the UniPrint Bridge that is required for centralized data access components. This component is required for SecurePrint, Email2Print and Print Route.
Email2Print	Installs the Email2Print components on the UniPrint Bridge. An instance of both the Data Server and Document Conversion Server are also required for Email2Print.
AUX_Server	Installs the Auxiliary Server components on the UniPrint Bridge which is required for Print Route and AirPrint printing.

Component	Description
Imprivata_Gateway	Installs the Imprivata Gateway components on the UniPrint Bridge and enables SecurePrint Imprivata authentication.
Data_Conversion_Server	Installs the Data Conversion Server components on the UniPrint Bridge and is required by Email2Print.
Print_Route	Installs the Print Route components on the UniPrint Bridge and enables Administrators to create printer replacement mappings for printers within user sessions. The Data_Server and AUX_Server components are also required.
Mobile_Print_Service	Installs the Mobile Print Service components on the UniPrint Bridge and enables printing from iOS, Android and Chrome OS mobile devices.
Print_Server	Installs the UniPrint Print Server components on Windows print servers.
SecurePrint_Components	Installs the SecurePrint components on the UniPrint Print Server.
IPPServer	Installs the AirPrint Printing Module on the UniPrint Print Server and enables Print Server-based printing for iOS and Mac OS devices.
App_Server	Installs the UniPrint Application Server components on the Citrix/RDS server or virtual desktop golden image. This component is required for client/server and print server-based printing.
Adobe_Plugin	Installs the Adobe Plug-in on the UniPrint Application Server and enables PDF printing from Adobe products without re-rendering.
Archive_Server	Installs the Archive Server components and enables automated archiving of print jobs.
Archive_Client	Installs the Archive Client on either the UniPrint Print Server to archive Gateway queue print jobs or the UniPrint Application Server to archive UniPrint queue print jobs.

Component	Description
Statistics_Server	Installs the Statistics Server components used to collect print job statistics from the Statistics Client.
Statistics_Client	Installs the Statistics Client on either the UniPrint Print Server to capture Gateway printer queue statistics and/or the UniPrint Application Server to capture UniPrint queue statistics. This component relays this capture data to the Statistics Server.

Example: `msiexec /q /i C:\UniPrint91_*.msi ADDLOCAL=Bridge,Administrative_Console,License_Server, PrintPAL_Server,SecurePrint_Server`

INSTALLDIR

Function: Specifies a custom installation path for the UniPrint program files.
Remarks: The full path specified must be enclosed in double quotation marks (“ ”) if spaces exist in the path.
Example: `msiexec /q /i C:\UniPrint91_*.msi ADDLOCAL=Bridge, Administrative_Console,License_Server,SecurePrint_Server INSTALLDIR=”C:\Program Files\UniPrint\Bridge”`

DOTNETVERSION 40CLIENT

Function: Enables or disables the requirement for .NET Framework 4.5 to be installed on the UniPrint Application Server, This requirement cna be disabled, if and only if the UniPrint Management Console is also not installed on the UniPrint Application Server.
Remarks: This command line parameter is used in conjunction with ADDLOCAL=*component*. If the Administrative_Console component is omitted then the requirement for .NET Framework 4.5 can be disabled by setting this parameter to 1.
Example: `msiexec /q /i C:\UniPrint91_*.msi ADDLOCAL=App_Server DOTNETVERSION40CLIENT=1`

UP_SETTING_ BRIDGEIP

Function: Specifies the IP address and port number of the UniPrint Bridge and/or license server.
Remarks: This parameter is only required during the UniPrint Print Server and UniPrint Application Server installation process. The IP address and the port number are both required. To specify the UniPrint Bridge with the default port number, 999, just type in the IP address with the colon (:) and the port number 999. For HA deployments, a second IP address can be added by using a comma.
Example: `msiexec /q /i C:\UniPrint91_*.msi ADDLOCAL=Print_Server,Administrative_Console, SecurePrint_Components UP_SETTING_BRIDGEIP=192.0.2.100:999`

HA Example: `msiexec /q /i C:\UniPrint91_*.msi ADDLOCAL=Print_Server,Administrative_Console, SecurePrint_Components UP_SETTING_BRIDGEIP=192.0.2.100:999, 192.0.2.101:999`

UP_SETTING _RUN_PRINTPAL

Function: Enables or disables the **Run PrintPAL on this server** option under **Logon options** in the **Sessions** screen of the UniPrint Management Console on the Application Server. This specifies whether or not to run the PrintPAL on this server. This is only available on the Application Server.
Remarks: If enabled, UPSession will automatically launch and run PrintPAL when a session is started. Default is 0 (Disabled).
Example: `msiexec /q /i C:\UniPrint91_*.msi ADDLOCAL=App_Server, Administrative_Console UP_SETTING_RUN_PRINTPAL=#1`

UP_SETTING_ PAPERSIZE=#n

Function: Specifies the default paper size for the UniPrint printer, UniPrint (Email PDF) and UniPrint (Save PDF) queues.
Remarks: Alternatively, this option can be set through the UniPrint Management Console on the UniPrint Application Server after installation is complete. A list of supported paper sizes can be found in "Paper Sizes" on page 425. The more common paper sizes are listed below.

n	Description
1	Letter (8.5 x 11 in)
5	Legal (8.5 x 14 in)
8	A3 (297 x 420 mm)
9	A4 (210 x 297 mm)

Example: `msiexec /q /i C:\UniPrint91_*.msi ADDLOCAL=App_Server, Administrative_Console UP_SETTING_PAPERSIZE=#9`

UP_SETTING_ UNIPRINT_AS_ DEFAULT

Function: Sets UniPrint as the default printer for all users when set to 1.
Remarks: Alternatively, this option can be set through the UniPrint Management Console on the UniPrint Application Server after installation is complete. Default is 1.
Example: `msiexec /q /i C:\UniPrint91_*.msi ADDLOCAL=App_Server, Administrative_Console #UP_SETTING_UNIPRINT_AS_DEFAULT=#0`

UP_SETTING_ GPO

Function: Specifies the order in which UniPrint applies settings from Active Directory Group Policy Objects.
Remarks: If a source is not specified, configurations from that source will not be applied. Do not use a comma or space between sources. The default order is UMD.

U	User Policy
M	Machine Policy

S	User Settings
D	Local Machine Settings

Example:
```
msiexec /q /i C:\UniPrint91_*.msi
ADDLOCAL=App_Server, Administrative_Console
UP_SETTING_GPO=MUD
```

UP_SETTING_LOGLEVEL=n

Function: Specifies the debugging log level for troubleshooting purposes.
Remarks: Alternatively, this option can be set through the UniPrint Management Console on the UniPrint Application Server after installation is complete. The default level is 1.

n	Description
0	None
1	Errors
2	Info
3	Debug (Full)

Example:
```
msiexec /q /i C:\UniPrint91_*.msi
ADDLOCAL=App_Server, Administrative_Console
UP_SETTING_LOGLEVEL=3
```

UP_SETTING_PASSTHROUGH=#n

Function: Disables or enables UniPrint pass-through.
Remarks: If enabled, UniPrint will treat this Application Server as a pass-through client, routing print jobs printed from another Application Server that also has the UniPrint Application Server component installed.

n	Description
1	RDP connections only
2	Legacy ICA (9.x and earlier) connections
3	RDP and Legacy ICA (9.x and earlier) connections
4	ICA 10.x and later connections only
5	RDP and ICA 10.x and later connections
6	Legacy ICA (9.x and earlier) and ICA 10.x and later connections
7	RDP, Legacy ICA (9.x and earlier), and ICA 10.x and later connections

Example:
```
msiexec /q /i C:\UniPrint91_*.msi
ADDLOCAL=App_Server, Administrative_Console
UP_SETTING_PASSTHROUGH=#5
```

UP_SETTING_NO_UNIPRINT_PRINTER

Function: Does not create the UniPrint printer queue when set to 1.
Remarks: This is recommended for SecurePrint implementations and is only applicable to the UniPrint Application Server. To recreate the UniPrint queue, change the OmitCreation value under registry key, HKEY_LOCAL_MACHINE\SOFTWARE\UniPrint\Control Service\Plugins\PRNINSTL\Printers\UniPrint to 0. The default is 0.

Example: `msiexec /q /i C:\UniPrint91_*.msi ADDLOCAL=App_Server, Administrative_Console UP_SETTING_NO_UNIPRINT_PRINTER=#1`

UP_SETTING_NO_SAVE_QUEUE

Function: Does not create the UniPrint (Save PDF) queue when set to 1.
Remarks: This only applies to the UniPrint Application Server. To recreate the UniPrint (Save PDF) queue, change the OmitCreation value under registry key, HKEY_LOCAL_MACHINE\SOFTWARE\UniPrint\Control Service\Plugins\PRNINSTL\Printers\UniPrint (Save PDF) to 0. The default is 0.
Example: `msiexec /q /i C:\UniPrint91_*.msi ADDLOCAL=App_Server, Administrative_Console UP_SETTING_NO_SAVE_QUEUE=#1`

UP_SETTING_VC_ORDER

Function: Sets the virtual channel order of detection in a session.
Remarks: This only applies to the UniPrint Application Server and can be changed after installation through the UniPrint Management Console.

t	RDP
c	ICA Virtual Channel
d	Client drive mapping
p	PCoIP
m	Mac client

Example: `msiexec /q /i C:\UniPrint91_*.msi ADDLOCAL=App_Server, Administrative_Console UP_SETTING_VC_ORDER=tcdm`

USE_VDI_SERVER_SETTINGS

Function: Sets whether or not to establish a static connection between the UniPrint Application Server and the UniPrint Bridge. This option is recommended for VDI environments.
Remarks: This only applies to the UniPrint Application Server. If set to 1, the UniPrint Application Server would only establish a connection to the UniPrint Bridge, when a print job is initiated. The default is 0.
Example: `msiexec /q /i C:\UniPrint91_*.msi ADDLOCAL=App_Server, Administrative_Console USE_VDI_SERVER_SETTINGS=1`

UP_SETTING_STAT_SERVICE_PORT

Function: Sets the port number that the Statistics Service is listening on.
Remarks: This only applies to the Statistics Server. To change the port number manually, change the ConnectionPort value under the registry key, HKEY_LOCAL_MACHINE\SOFTWARE\UniPrint\Statistics Service. The default port number is 10308.
Example: `msiexec /q /i C:\UniPrint91_*.msi ADDLOCAL=Statistics_Server,Administrative_Console UP_SETTING_STAT_SERVICE_PORT=#12345`

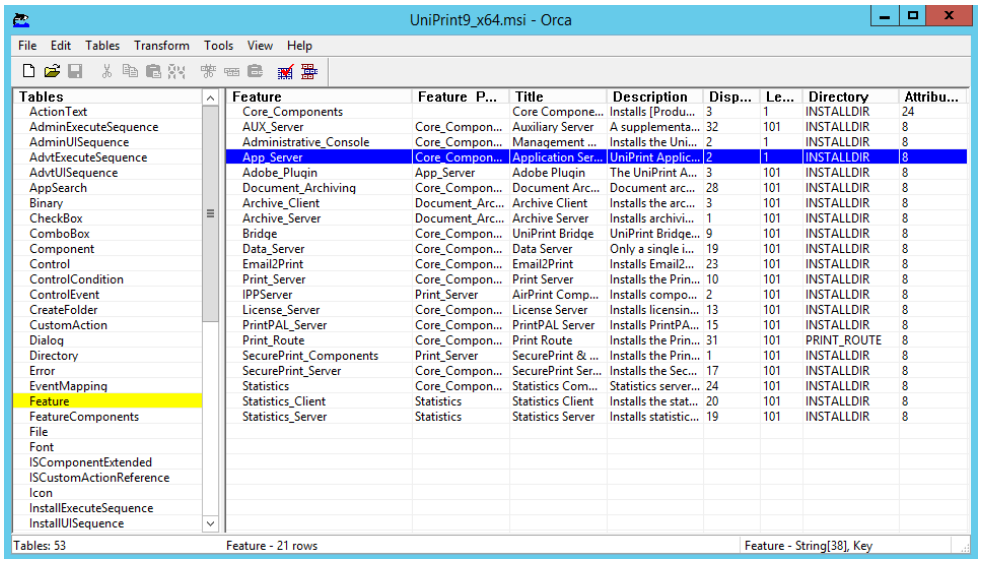
UP_SETTING_STAT_CLIENT_PORT

Function: Sets the port number that the Statistics Client Service is listening on.
Remarks: This only applies to the Statistics Client. To change the port number manually, change the ConnectionPort value under the registry key, HKEY_LOCAL_MACHINE\SOFTWARE\UniPrint\Statistics Client Service. The default port number is 10309.
Example: `msiexec /q /i C:\UniPrint91_*.msi ADDLOCAL=Statistics_Client,Administrative_Console UP_SETTING_STAT_CLIENT_PORT=#12345`

Using Group Policy to Deploy UniPrint Remotely

The following instructions are based on Windows Server 2012 R2 and assumes that the following have been created: a Group Policy Object and distribution point (both of which must be accessible by the domain controller), the UniPrint Bridge, the UniPrint Print Server, the UniPrint Application Server, and virtual desktop images, on which you wish to have UniPrint components installed.

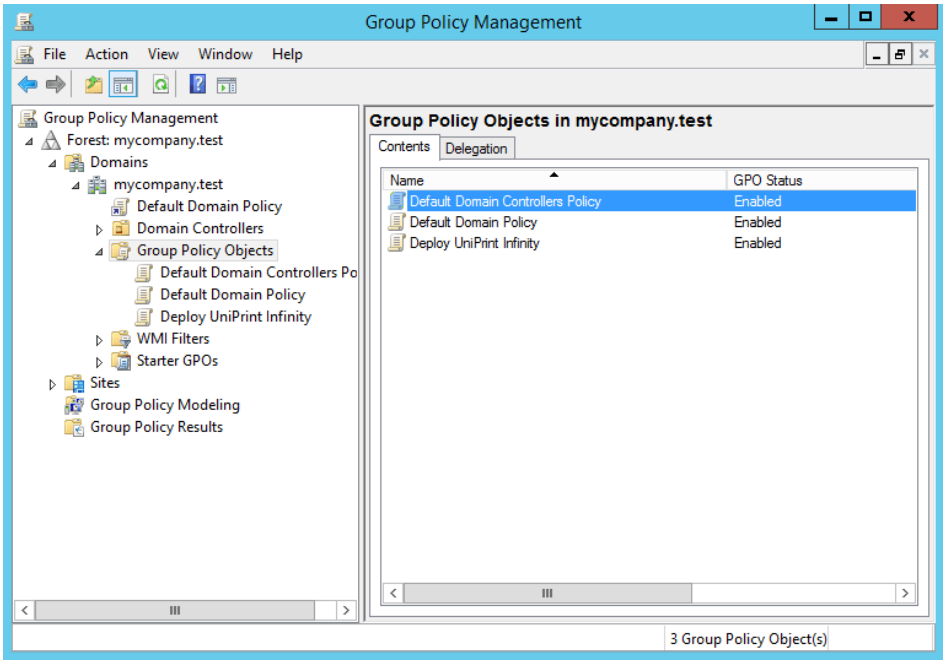
Standard transform (.MST) files are included in the UniPrint installation package and are located in \\Admin\Transforms. These transform files only include the more commonly used basic features. For custom installations, a new transform file can be created with Orca by setting the features **Level** to **1**.



To deploy UniPrint91_*.msi through Group Policy Management, do the following for each UniPrint component:

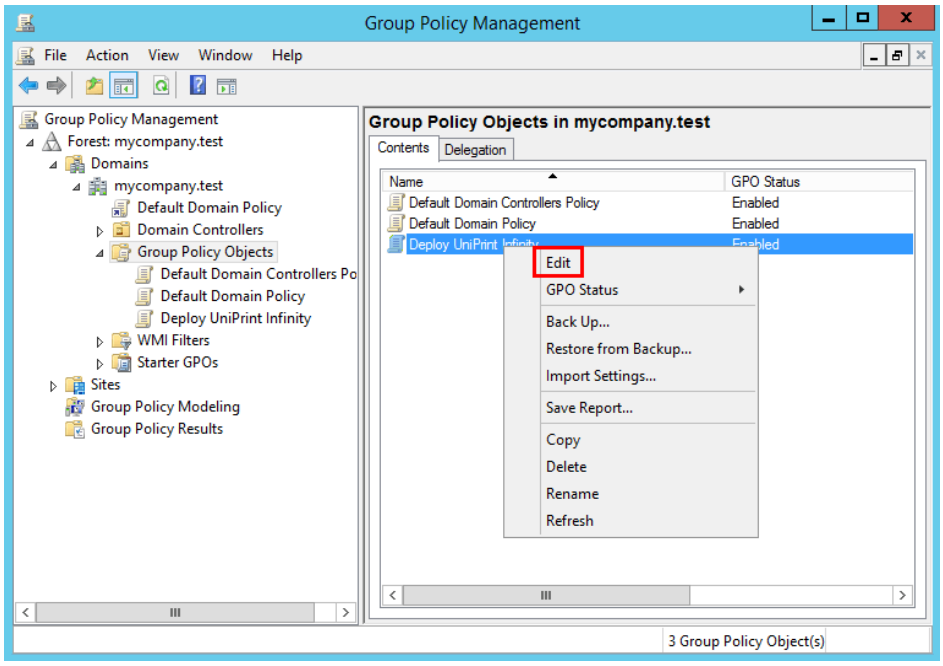
1. From your domain controller, click **Start**, click the **Administration Tools** tile and then click **Group Policy Management**.

2. Expand the domain containing the server devices and virtual desktop images to which you want to deploy UniPrint and then click **Group Policy Objects**.

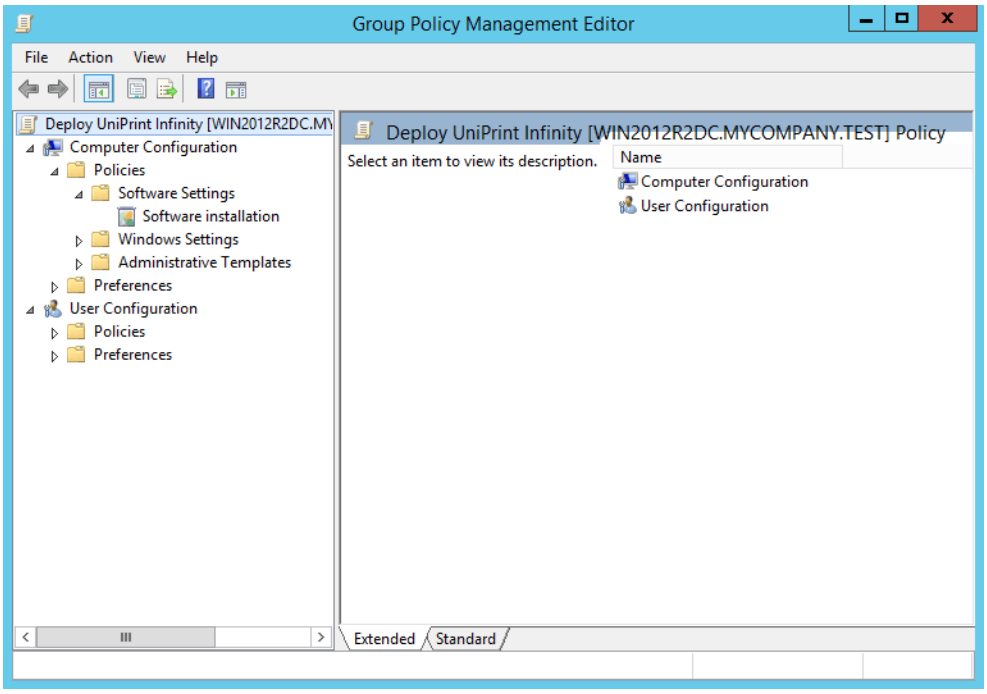


NOTE: Applying this software installation policy at the domain level will result in UniPrint Infinity being deployed to all devices with Windows 2003 or later, including client devices.

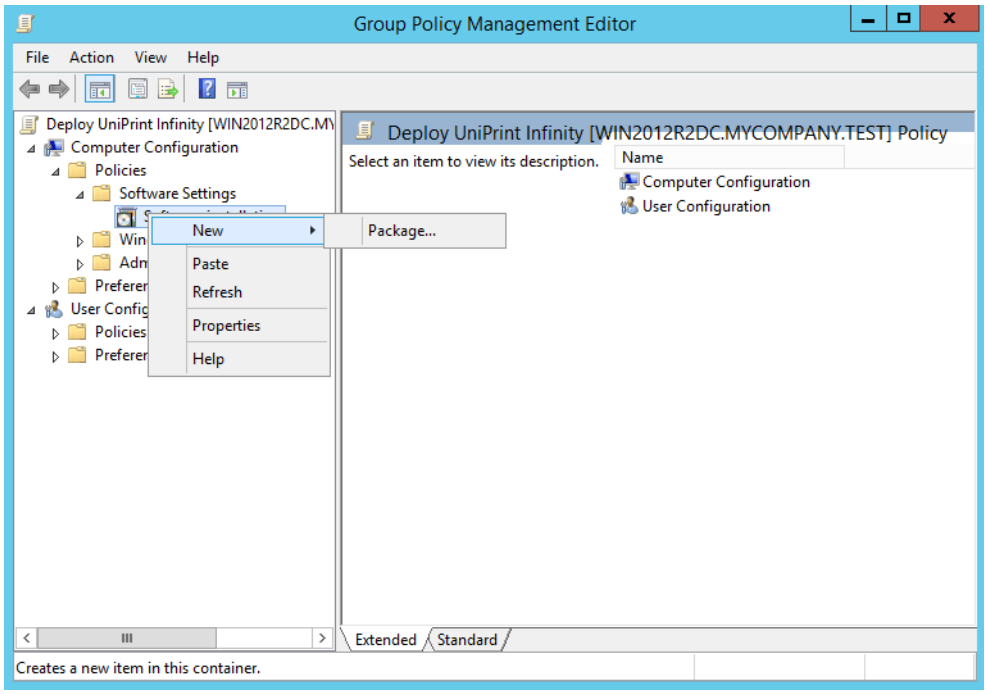
3. Right-click the group policy object that you want to use to deploy UniPrint Infinity, and then select **Edit.**



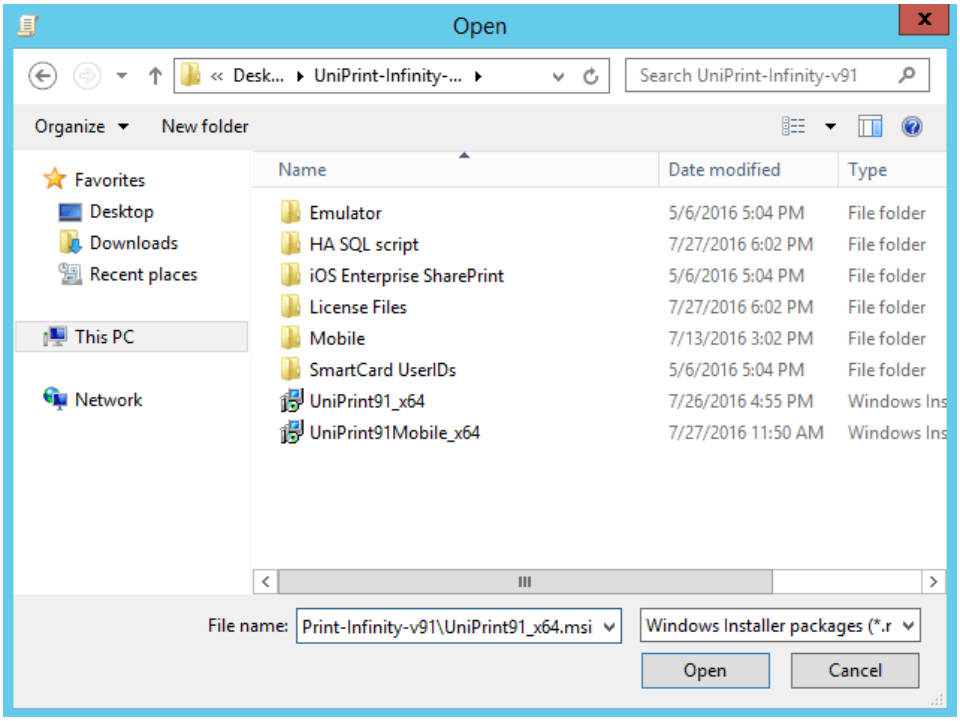
4. Under **Computer Configuration**, expand **Policies** and then **Software Settings**.



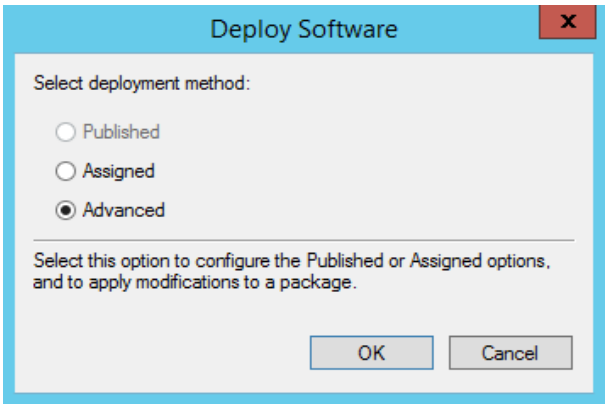
5. Right-click **Software Installation**, point to **New**, and then click **Package**.



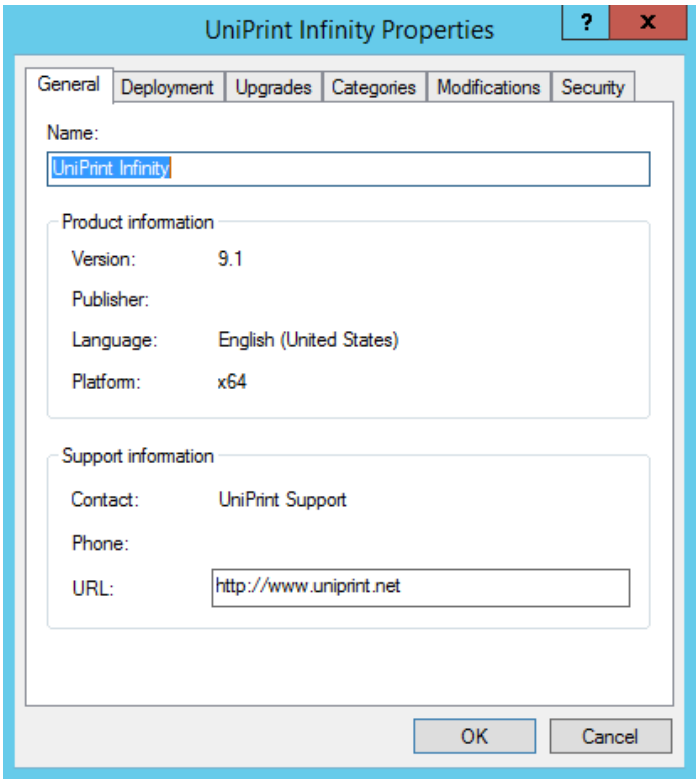
6. In the **Open** dialog box, type the full Universal Naming Convention (UNC) path of the UniPrint91_*.msi package, for example, `\\file_server\share\UniPrint91_*.msi`. Click **Open**.



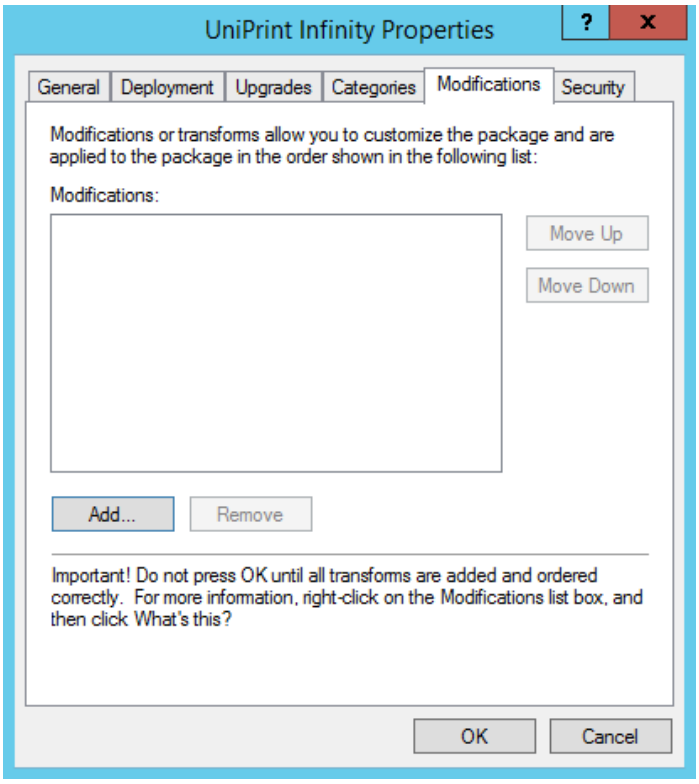
7. In the **Deploy Software** dialog box, select **Advanced,** and then click **OK**.



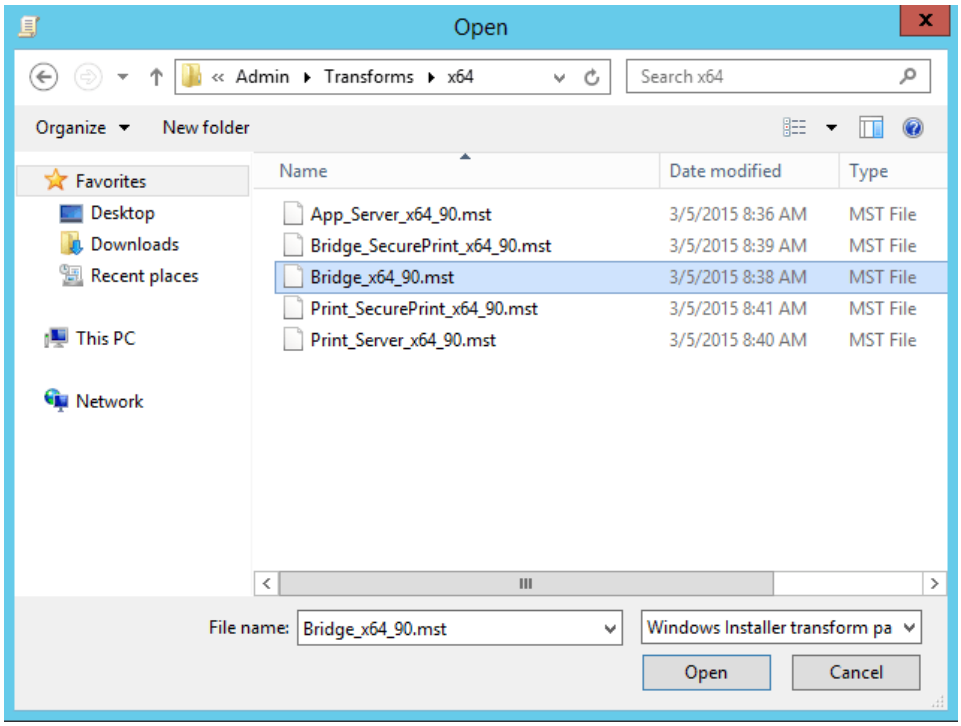
8. In the **UniPrint Infinity Properties** dialog box, click the **Modifications** tab.



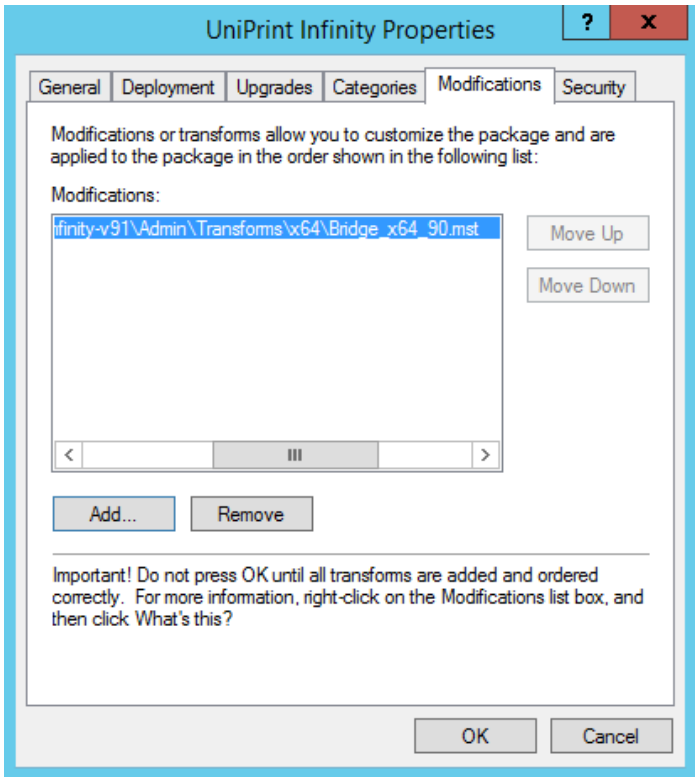
9. Click **Add** to add the transform file.



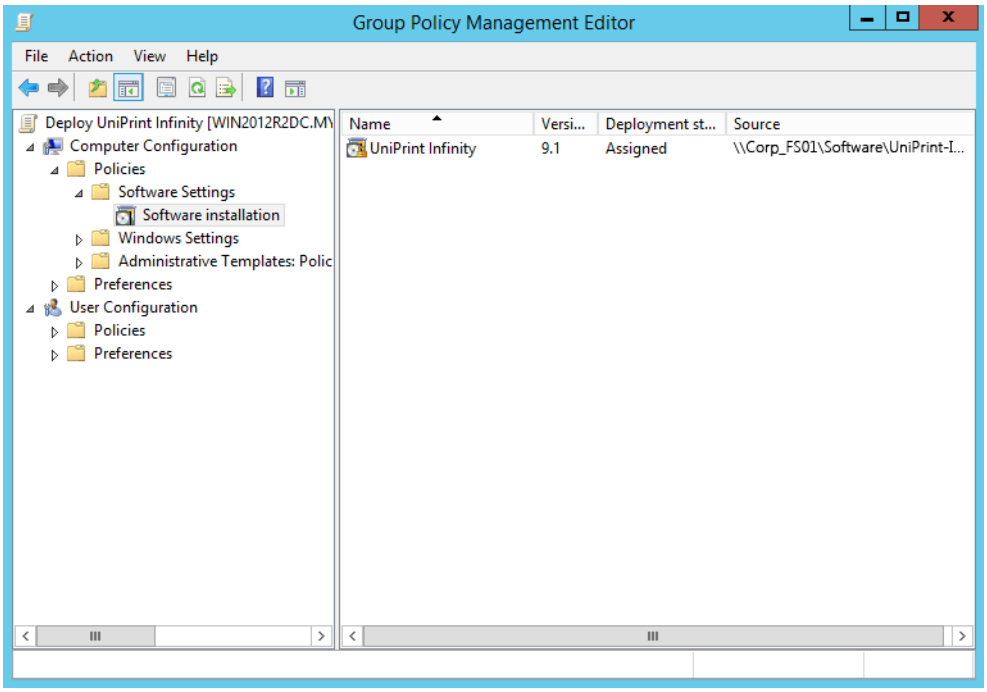
10. Click to select the desired transform (.mst) file and then click **Open**.



11. Click **OK**.



12. UniPrint will now appear in the right pane of the **Group Policy** window.



13. Close the Group Policy Management Editor and then close the Group Policy Management snap-in.

Modifying & Removing UniPrint

Before proceeding ensure that *all user sessions have ended*, and that new logons to the application server or virtual desktop image have been disabled. Removing UniPrint Infinity components *requires that the server be restarted* to release files locked by the operating system.

Modifying a UniPrint Installation

To modify a UniPrint Infinity installation, you must either be logged in as the built-in "Administrator" or you must have UAC disabled. By design, modifying UniPrint Infinity as a user with administrative privileges does not give you sufficient permissions.

1. Click **Start** and then click the **Control Panel** tile.

2. Click **Programs and Features**.

3. From the list of installed applications, click to select **UniPrint Infinity** and then click **Change**.

4. In the **UniPrint Infinity Maintenance** dialog box, click **Next**.

5. In the **Program Maintenance** dialog box, select **Modify** and then click **Next**.

6. In the **Custom Setup** dialog box, add or remove the desired components and then click **Next**.

7. If you are modifying UniPrint Infinity on a server other than the Bridge, the **UniPrint Bridge Configuration** dialog box will be presented. Enter or confirm that the IP address of the UniPrint Bridge is correct and then click **Next**.

8. In the **Ready to Modify the Program** dialog box, click **Install**.

9. Click **Finish** to complete the modifications.

Removing UniPrint

To remove UniPrint Infinity completely from your environment, the following procedure must be performed on all UniPrint Infinity component servers.

1. Click **Start** and then click **Control Panel**.

2. Click **Programs and Features**.

3. From the list of installed applications, click to select **UniPrint Infinity** and then click **Uninstall**.

4. Click **Yes** to confirm that you want to remove UniPrint Infinity.

5. Click **OK** and then restart the server.

CHAPTER 3

UniPrint Infinity

Configuring UniPrint Bridge

Most of the configuration for UniPrint Infinity is done through the UniPrint Management Console. Although most settings can be changed from any UniPrint Infinity component, initial configuration should be performed from the suggested component.

On the UniPrint Bridge, administrators have the ability to change the default Gateway printer properties, delete or pause an available Gateway printer and create new FTP printer instances. This is also where you would initially configure PrintPAL, SecurePrint, Printer Delegation, and Print Route.

Since the License Server component cannot be installed without the UniPrint Bridge component, obtaining and then applying a license to the License Server also falls under this server.

Obtaining and Applying a UniPrint Infinity License

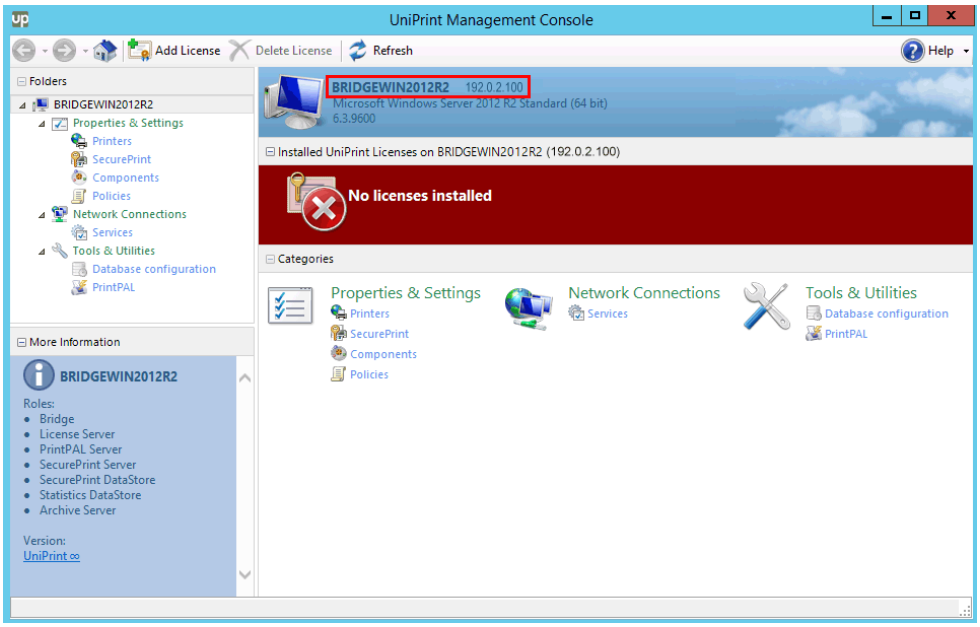
A license file is required for UniPrint Infinity to produce print jobs without a watermark printed across each page. This file is a registry file that needs to be imported to the UniPrint Bridge that is also the designated license server.

Obtaining a UniPrint License

1. Log on to the UniPrint Bridge machine that has the license server component installed.

2. Open the **UniPrint Management Console**.

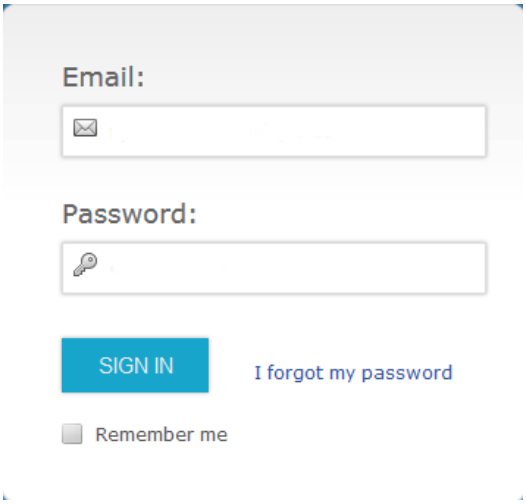
3. The top banner displays the license server's information. Take note of the server's IP address and host name.



NOTE: In a dual NIC environment, UniPrint will detect the first NIC address reported.

4. Go to the UniPrint Web site, www.uniprint.net. Click **Sign In**. If you are a new customer, click **Register**. Complete the form and then click **Register**.

5. For returning users, enter your credentials and then click **SIGN IN**.



6. To add a license, click **Add License**. An e-mail with a unique serial number was sent when you purchased UniPrint Infinity.

7. Enter the Serial Number (from the e-mail), UniPrint Bridge **Server Name** and **Server IP Address** information.

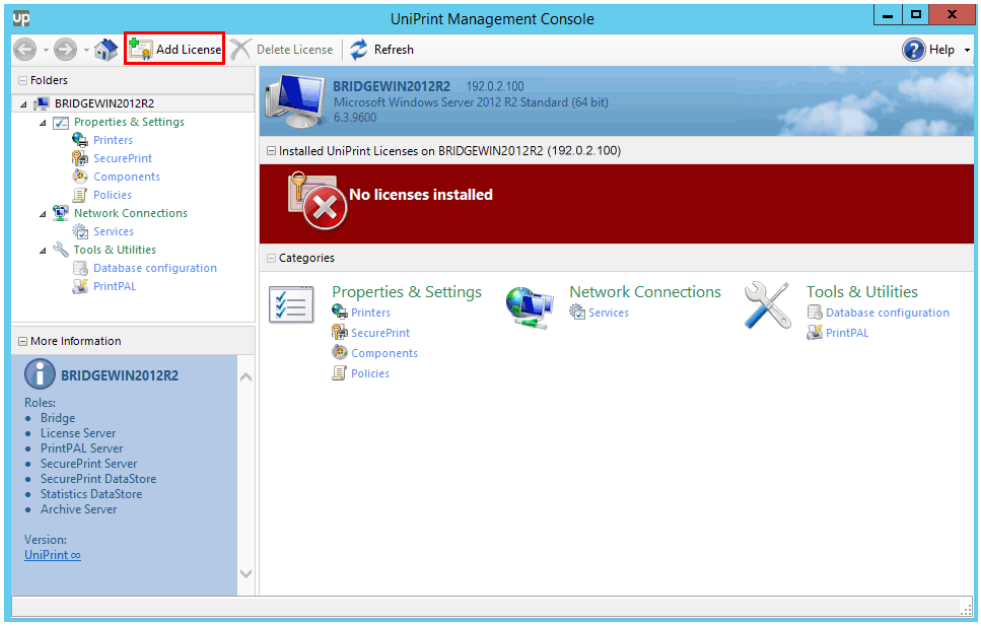
8. Click **Add** and a license file will be sent to the e-mail address used for signing in. Follow the instructions in the e-mail message to change the attached file from a *.txt file to a *.reg file.

NOTE: The license file is sent electronically from support@uniprint.net. To ensure this message is received, verify that anti-spam filters are not blocking messages from this e-mail address.

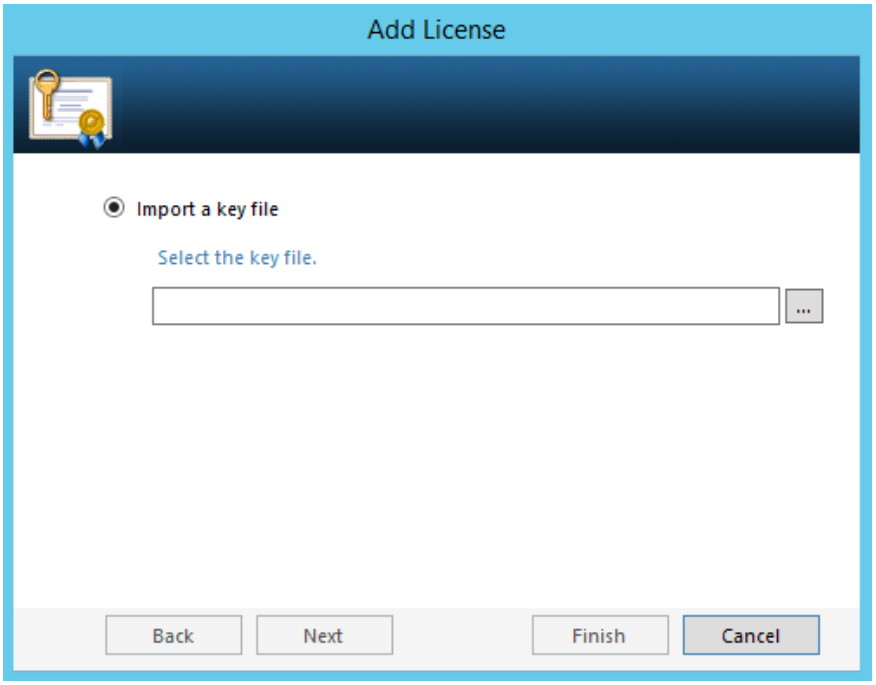
Applying a UniPrint License

1. On the UniPrint Bridge (License Server), open the **UniPrint Management Console**.

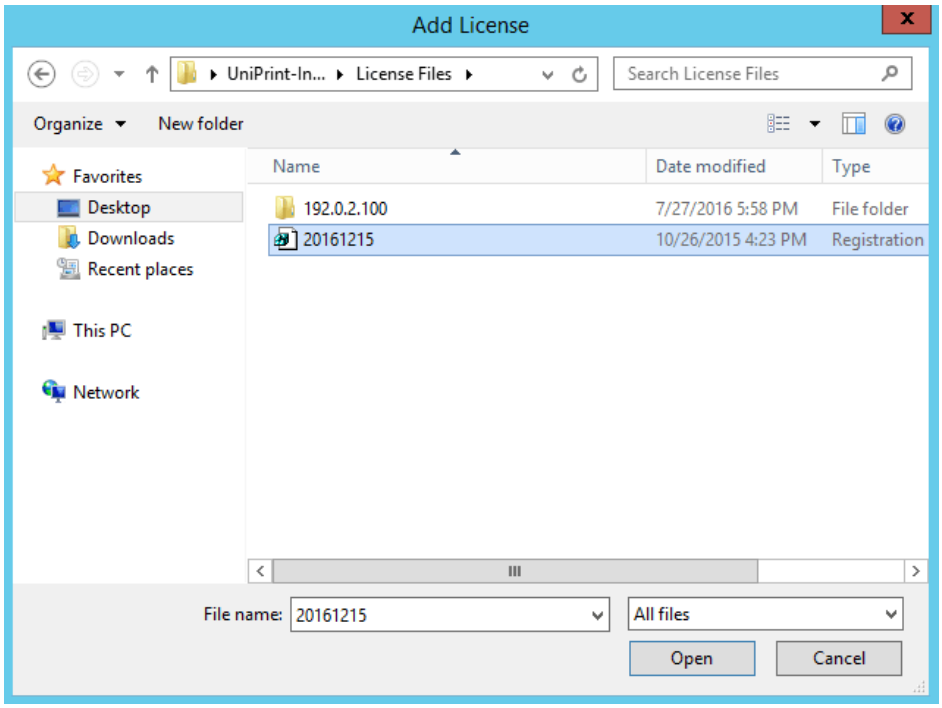
2. Click **Add License.**



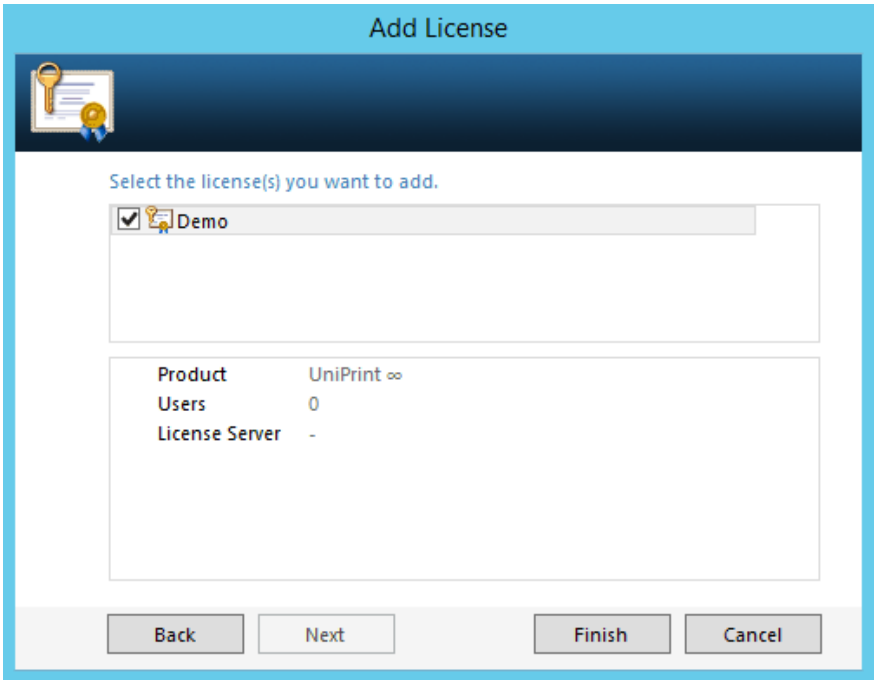
3. Click ... to browse for the UniPrint License file (*.reg).



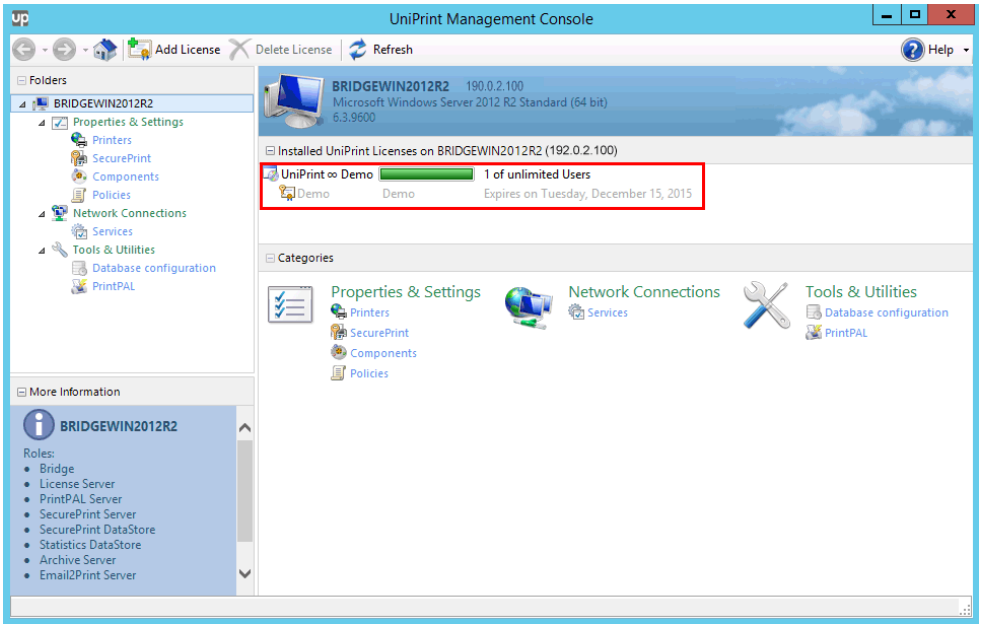
4. Click the license file and then click **Open**.



5. Select the license you want to add and then click **Finish**.



6. The license information should appear under the top banner.

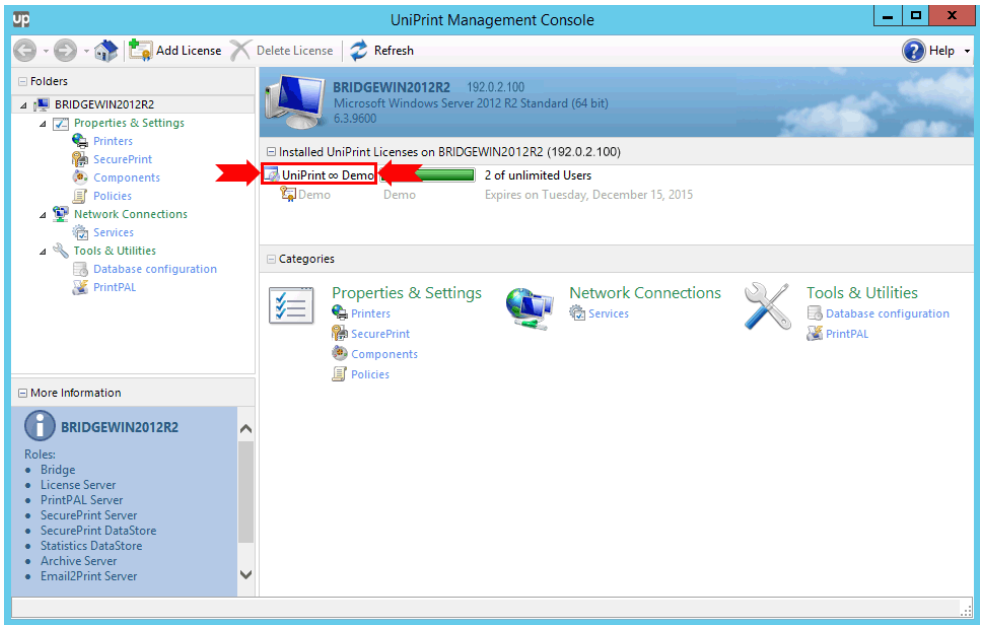


Viewing and Saving a Snapshot of License Usage

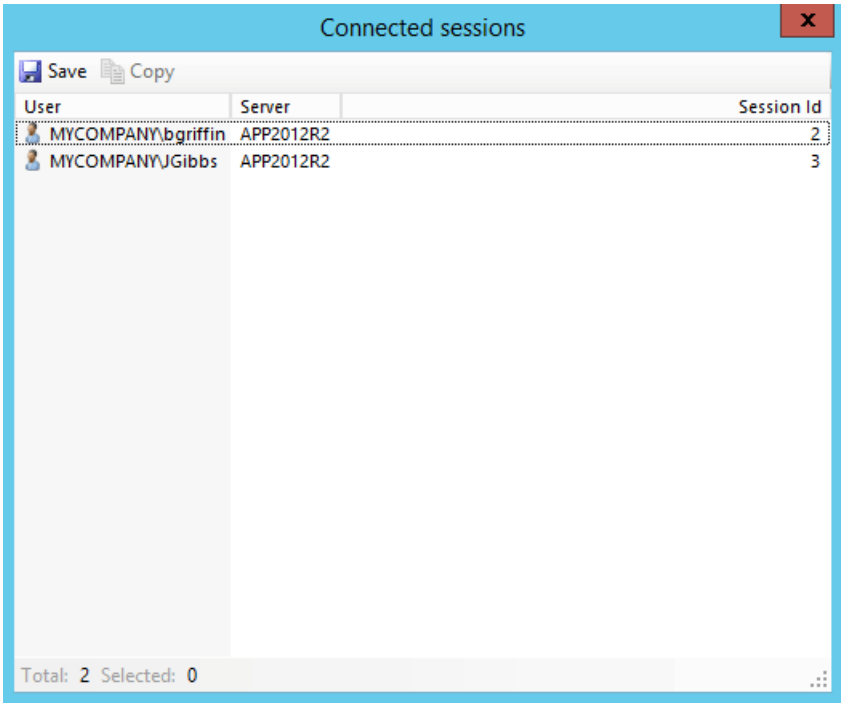
Viewing a Snapshot of License Usage

1. On the UniPrint Bridge (License Server), open the **UniPrint Management Console**.

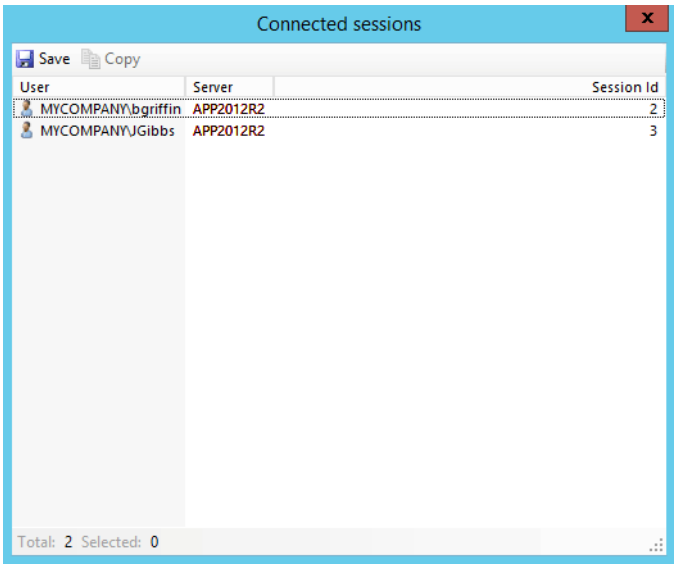
2. Under **Installed UniPrint Licenses on [*Bridge*] ([*Server IP Address*])**, double-click the license.



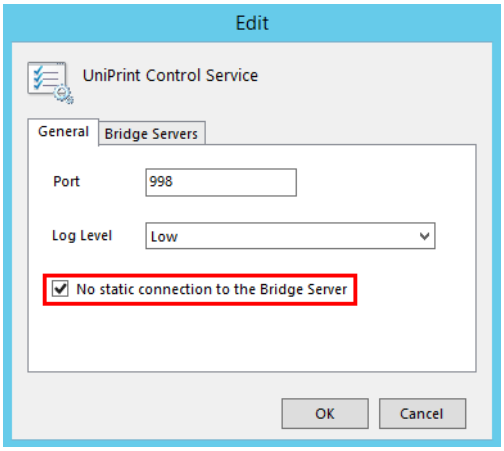
3. A list of users, the license type, the application server they are logged onto and their session IDs will appear. ***Note**: This is only a snapshot. Users that log in afterwards will not be reflected in this view.*



NOTE: Server host names will appear red when there is no communication between the UniPrint Bridge and the UniPrint Application Server.



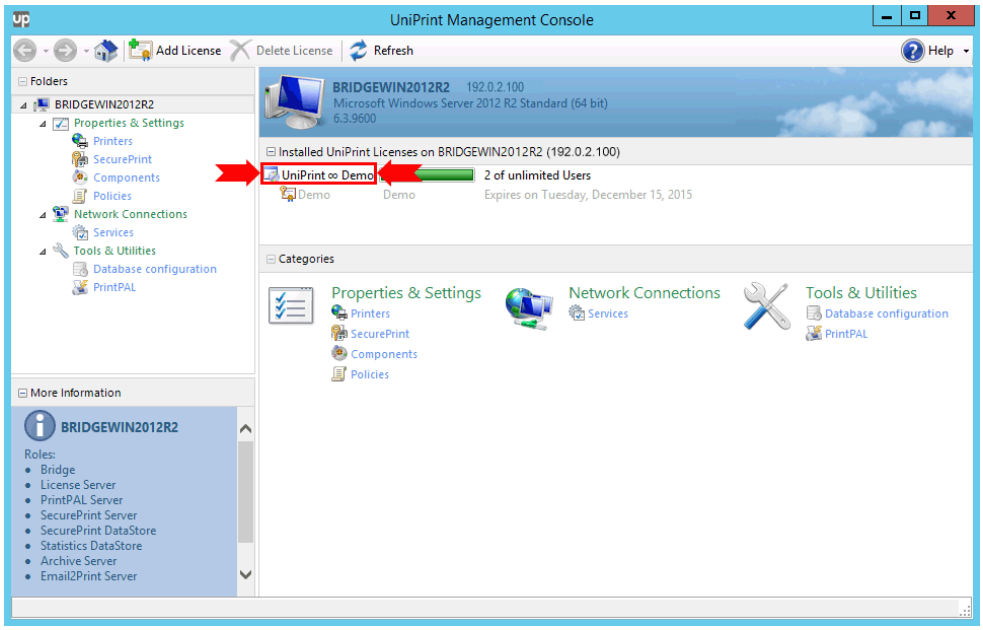
In a VDI environment, this may be due to the No static connection to the Bridge Server option being enabled.



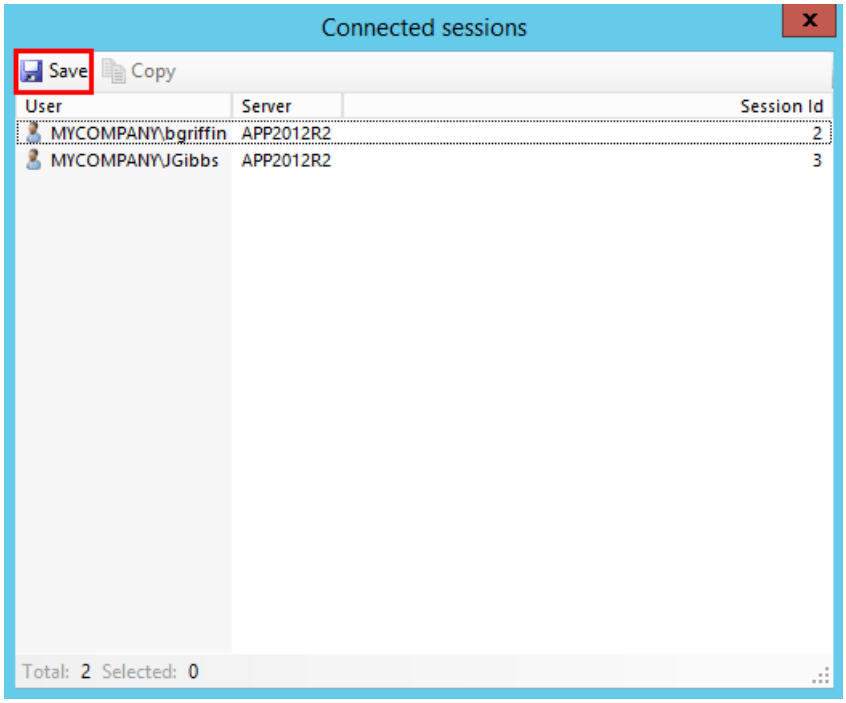
Saving a License Usage Snapshot To a File

1. On the UniPrint Bridge (License Server), open the **UniPrint Management Console**.

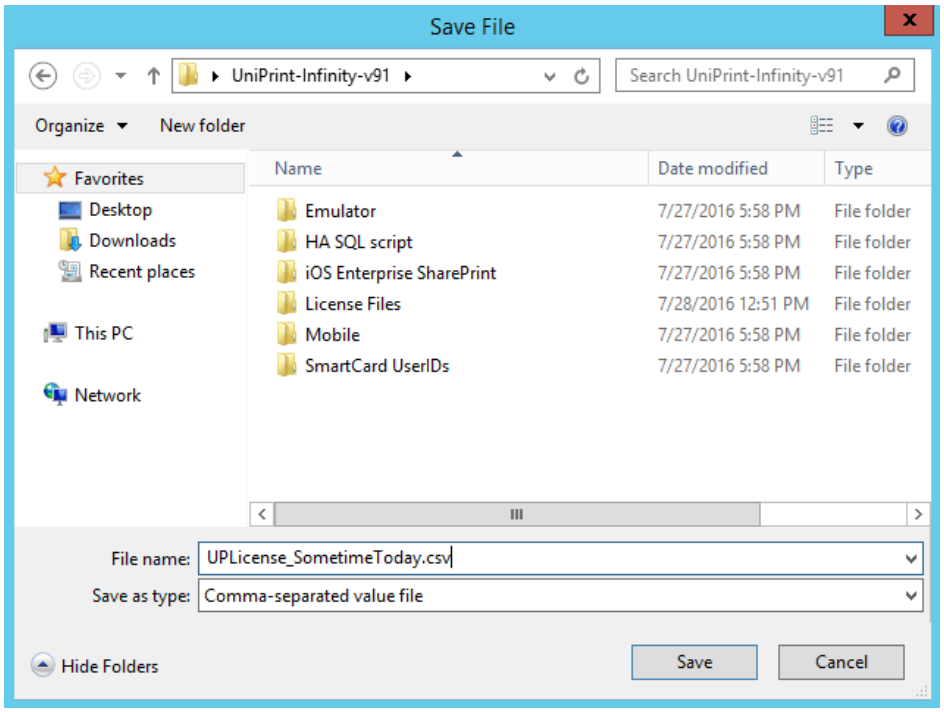
2. Under **Installed UniPrint Licenses on [*Bridge*] ([*Server IP Address*])**, double-click the license.



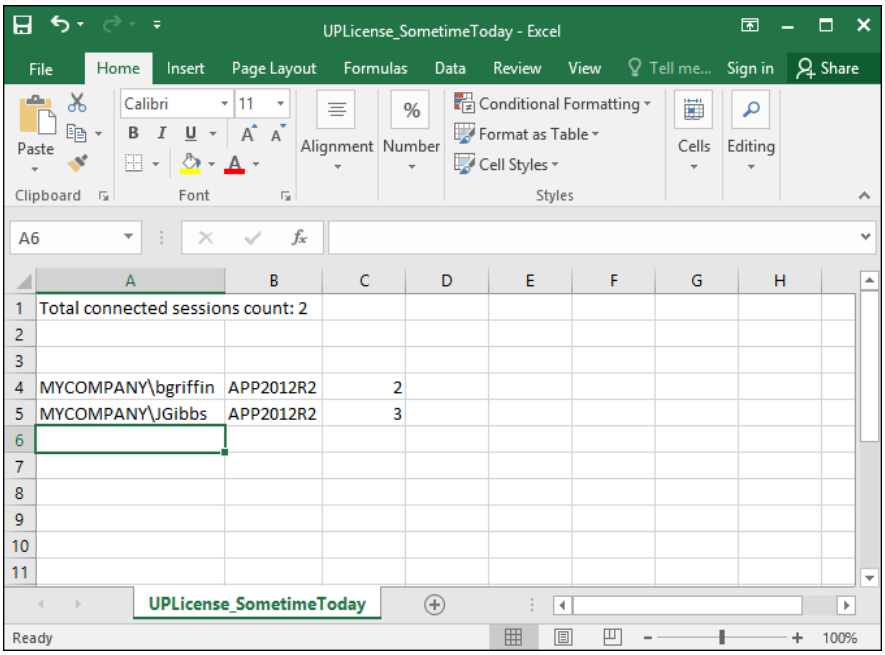
3. In the **Connected sessions** dialog box, click **Save**.



4. In the **Save File** dialog box, select a destination to save to and then type a file name. Click **Save**.



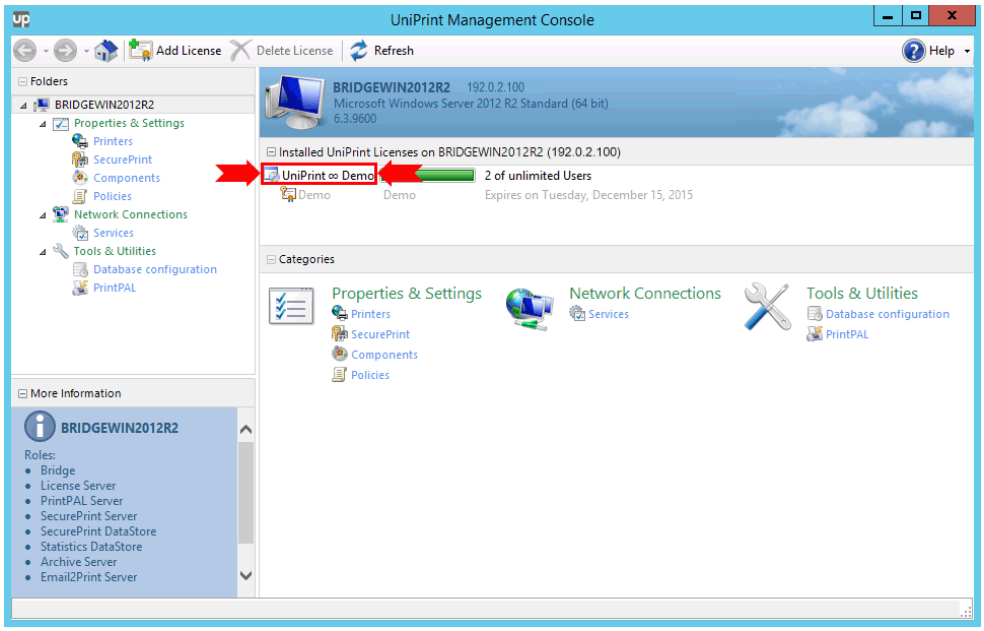
5. The file will be saved as a .CSV file. This file can be opened in Microsoft Excel.



Copying a License Usage Snapshot to the Clipboard

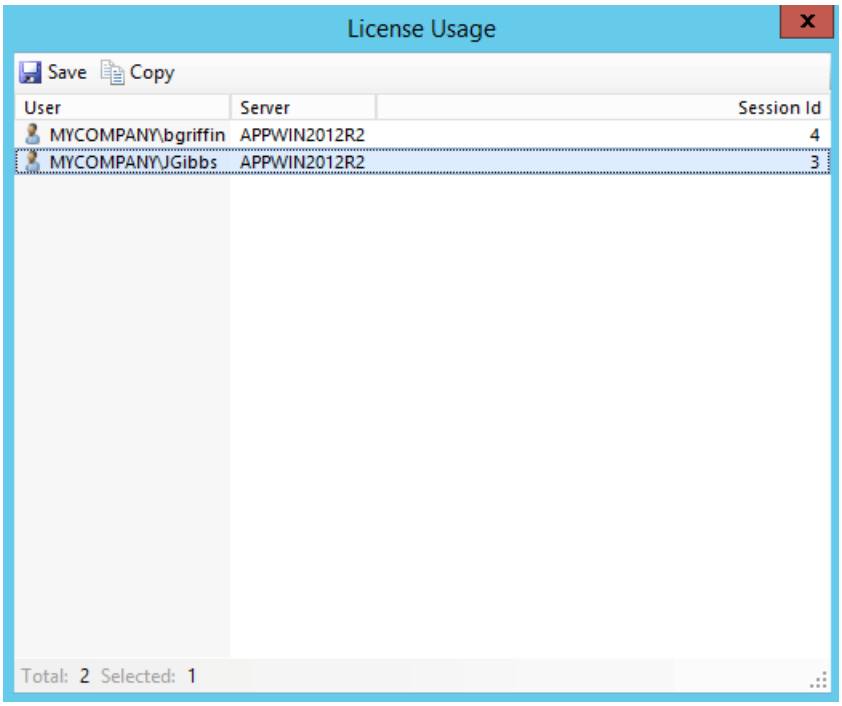
1. On a UniPrint Bridge (License Server), open the **UniPrint Management Console**.

2. Under **Installed UniPrint Licenses on [*Bridge*] ([*Server IP Address*])**, double-click the license.



3. In the **Connected sessions** dialog box, click to select the entry to copy. To select multiple entries, hold down **CTRL** and then click an

entry. For adjacent entries, hold down **SHIFT**, click the first entry and then click the last entry. Click **Copy**.



4. This information can be pasted into Microsoft Excel or another preferred application.

Setting License Thresholds & Alerts

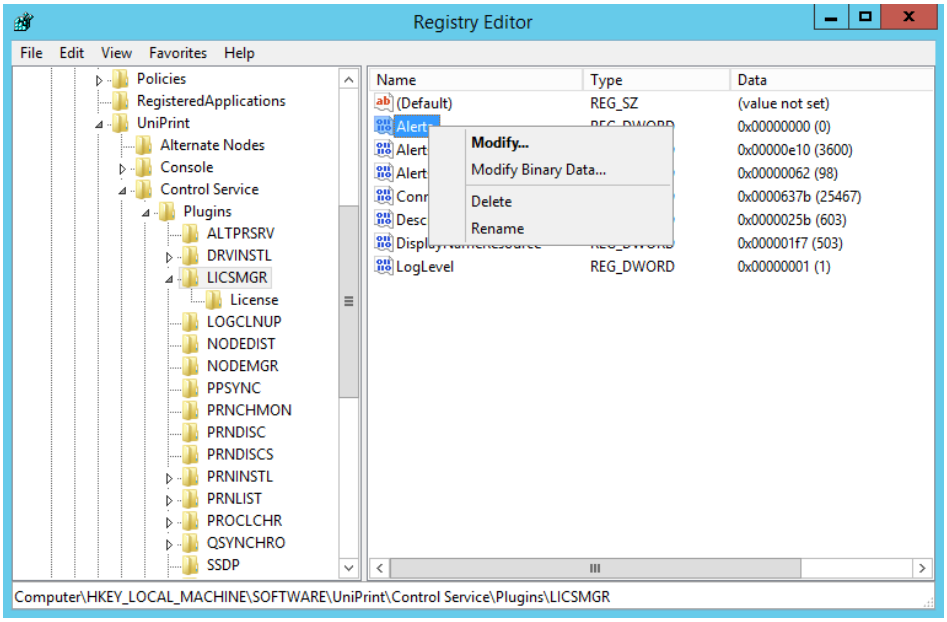
When the total license usage reaches a specified level, UniPrint Infinity can be configured to create an event in Windows Event Viewer. An e-mail is not sent automatically and requires the administrator to set it up manually when the event is triggered.

Enabling Licensing Alerts

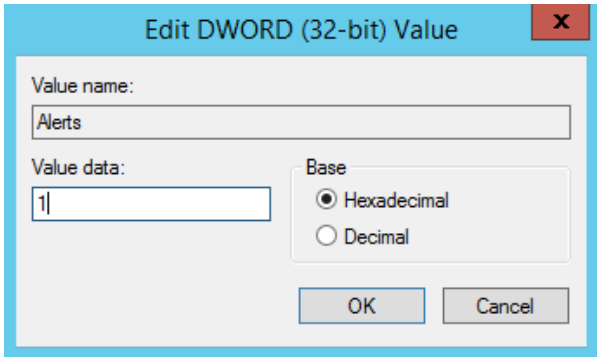
Licensing alerts are disabled by default. To enable licensing alerts, do the following:

1. On the License Server, open the registry editor.

2. Under the key, **HKEY_LOCAL_MACHINE\SOFTWARE\UniPrint\Control Service\Plugins\LICSMGR**, right-click the registry value, **Alerts**, and then click **Modify**.



3. Set the value to **1** and then click **OK**.

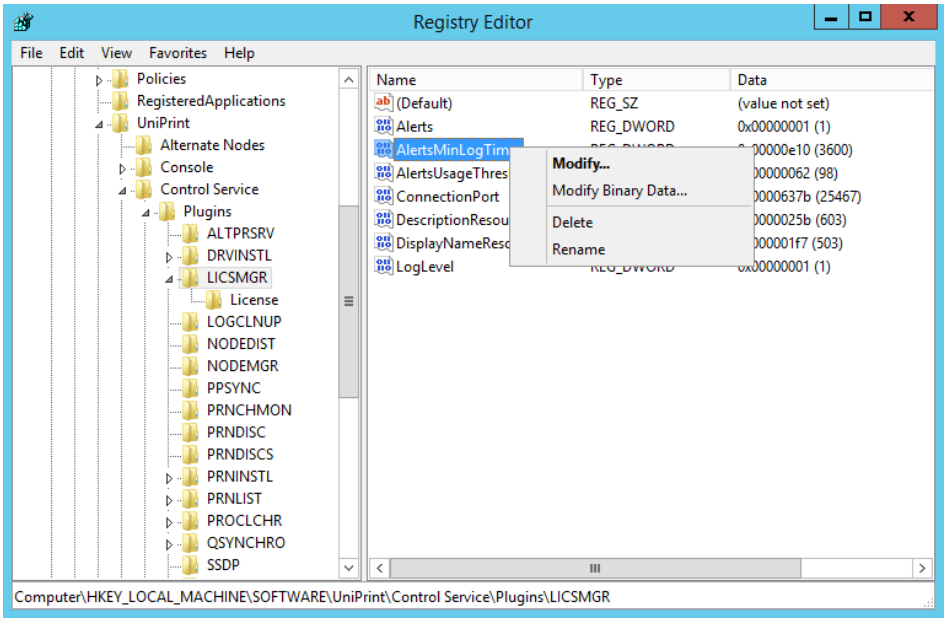


Changing Licensing Alerts Frequency

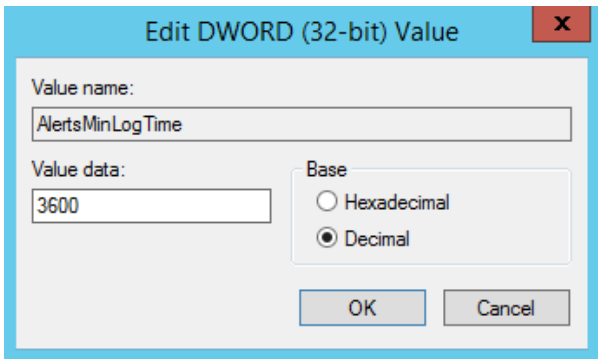
Licensing alerts are set to create an event in the Windows Event Viewer every 3600 seconds by default. To change the frequency of licensing alert creation, do the following:

1. On the License Server, open the registry editor.

2. Under the key, **HKEY_LOCAL_MACHINE\SOFTWARE\UniPrint\Control Service\Plugins\LICSMGR**, right-click the registry value, **AlertsMinLogTime**, and then click **Modify**.



3. Set the value in seconds, for example, 3600 seconds for 1 hour and then click **OK**.

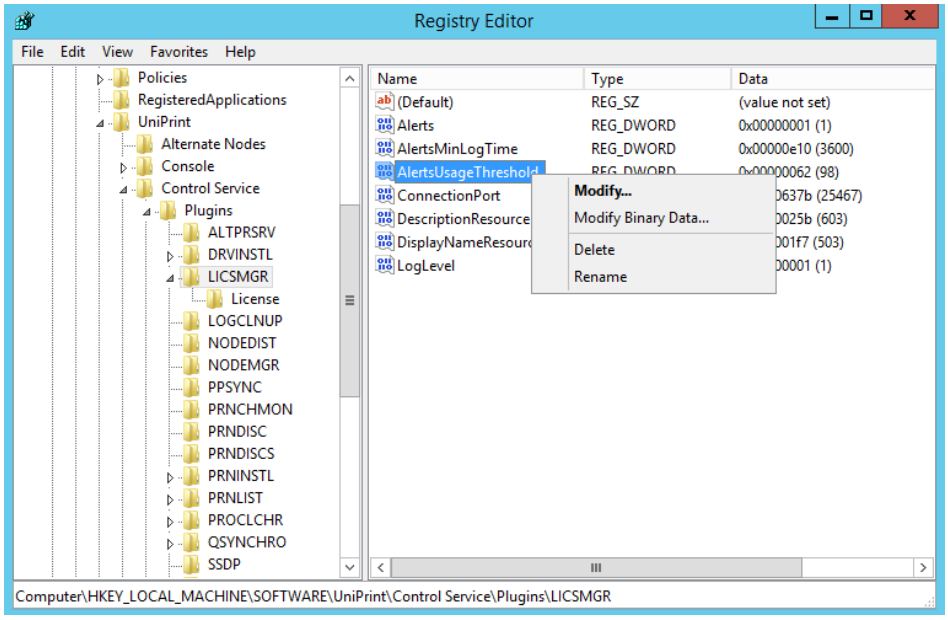


Setting the License Threshold

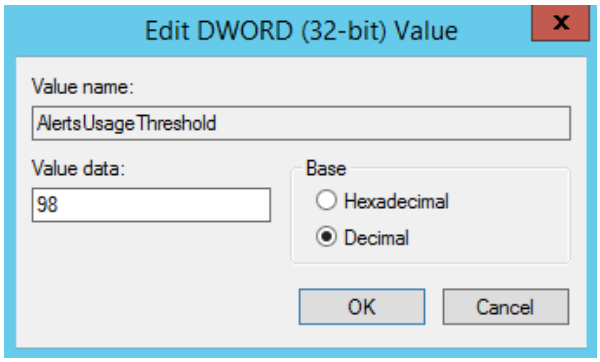
To change license threshold, do the following:

1. On the License Server, open the registry editor.

2. Under the key, **HKEY_LOCAL_MACHINE\SOFTWARE\UniPrint\Control Service\Plugins\LICSMGR**, right-click the registry value, **AlertsUsageThreshold**, and then click **Modify**.

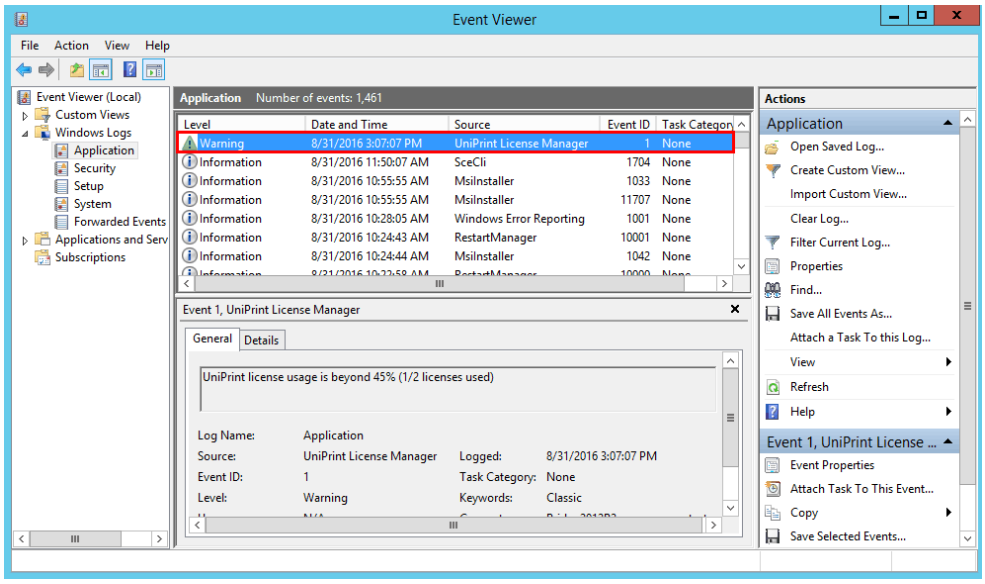


3. Set the value as a percentage and then click **OK**. By default the value is set to 98%.



Creating a Task to Send an E-mail When An Exceeded Threshold Event is Triggered

When license usage exceeds the threshold, an event is logged in the Event Viewer.



Using this event log, a task can be created to send an e-mail to an administrator. This can be accomplished using a PowerShell script and Task Scheduler.

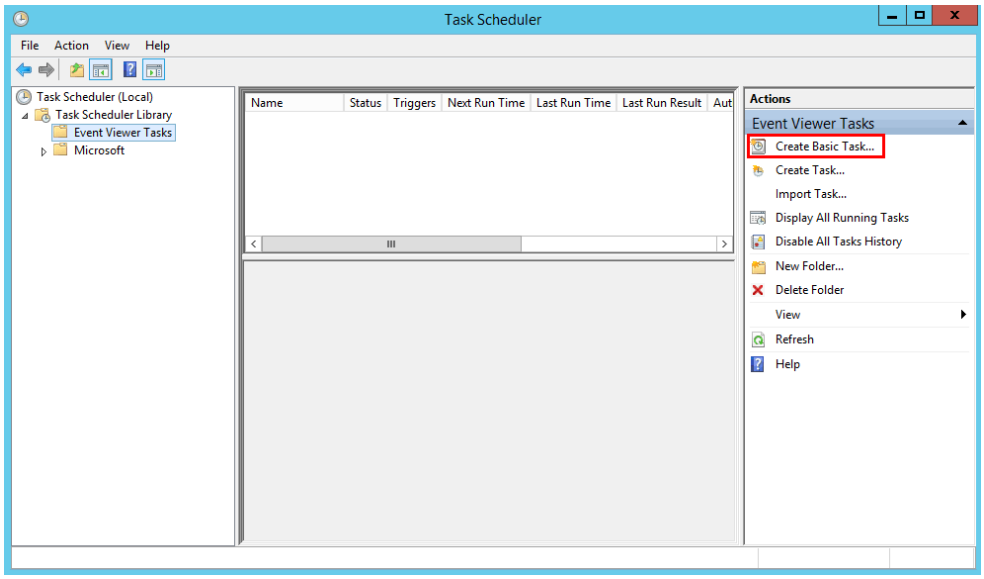
1. Open **Notepad** and create a PowerShell script similar to the one below.

```
Send-MailMessage -to <recipient_email_address> -Subject
   "UniPrint License Usage Threshold Exceeded" -body "Error
   1 License Server Manager. UniPrint license usage
   threshold alert was generated on server. Please
   investigate." -smtpserver <your_mail_server> -from
   <sender_email_address>
```

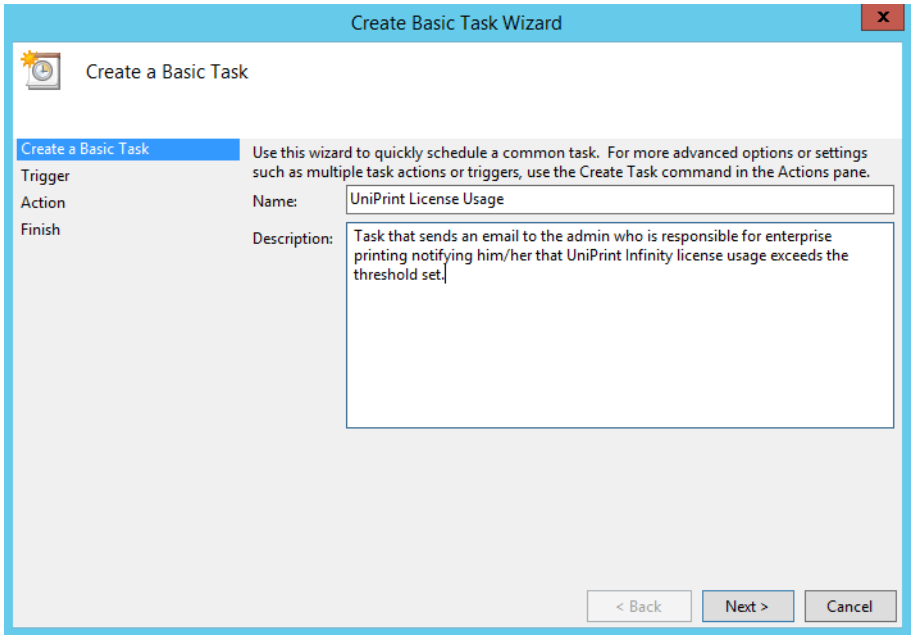
2. Save the script as **SendUPEmail.ps1** to an accessible location, for example, `C:\Scripts\SendUPEmail.ps1`.

3. Open **Task Scheduler**, expand **Task Scheduler Library** and then click to select **Event Viewer Tasks**.

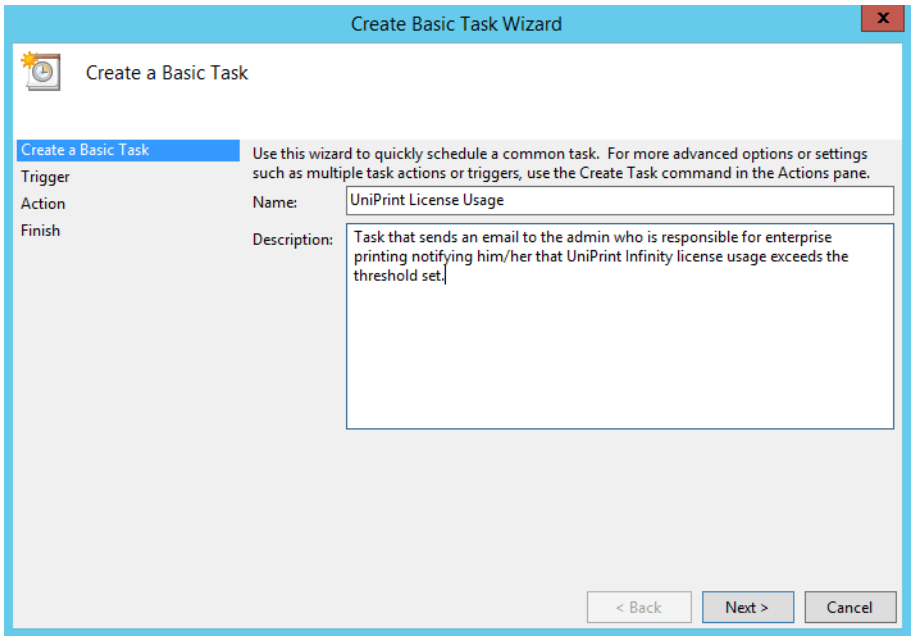
4. Under **Actions**, click **Create Basic Task**.



5. In the **Create a Basic Task** dialog box, enter a name and description for the task and then click **Next**.



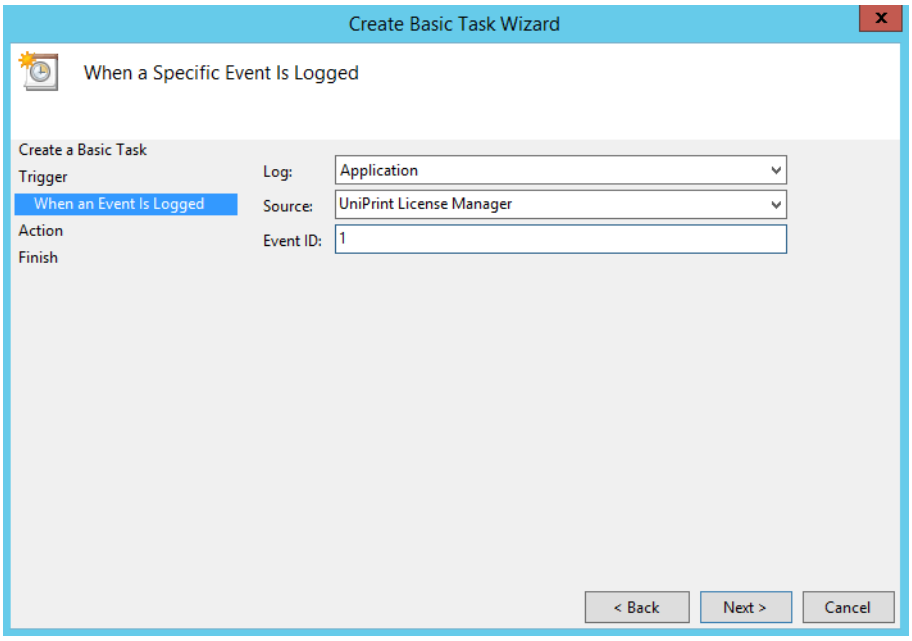
6. Click **When a specific event is logged** and then click **Next**.



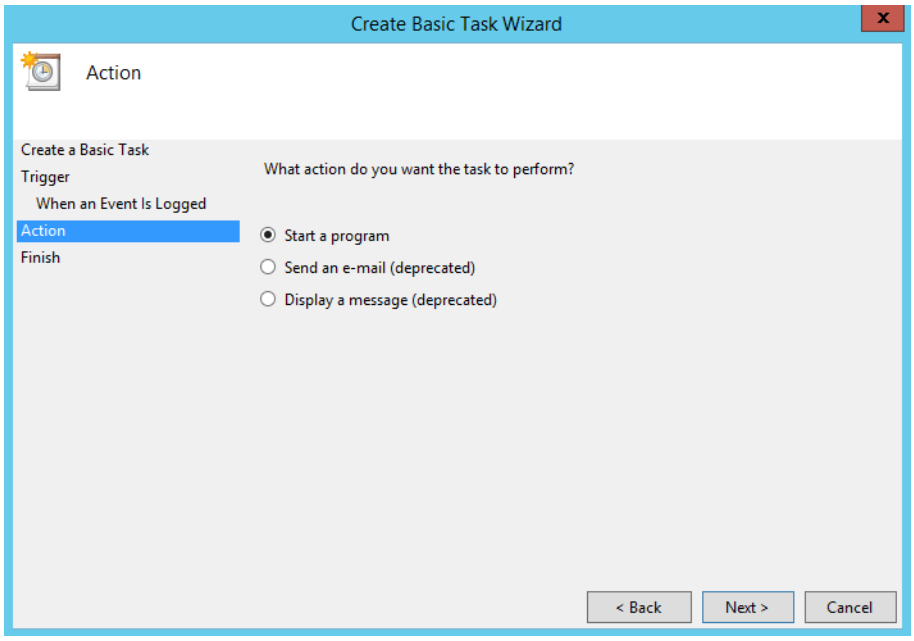
7. From the **Log** list, select **Application**.

8. From the **Source** list, select **UniPrint License Manager**.

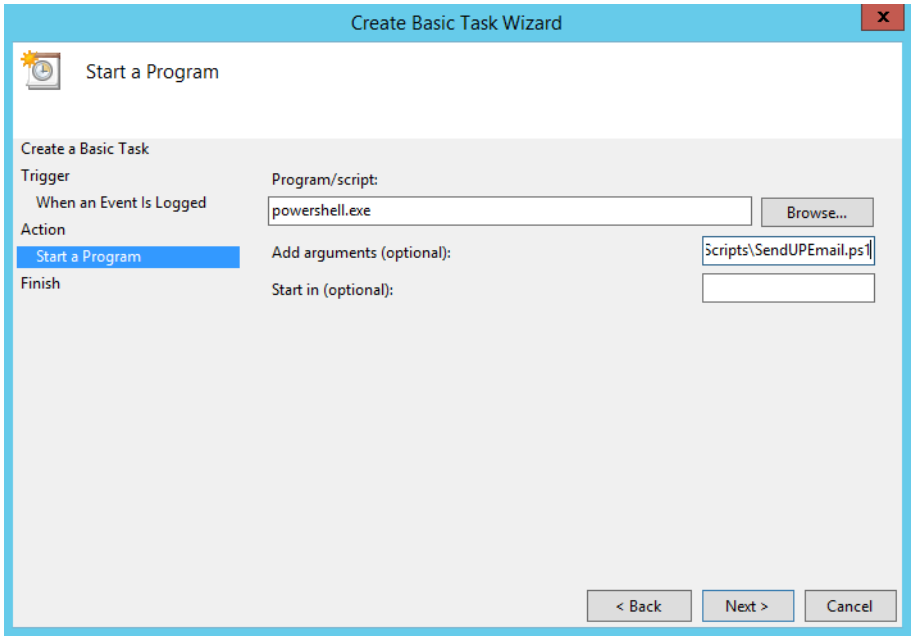
9. For the **Event ID**, enter **1** and then click **Next**.



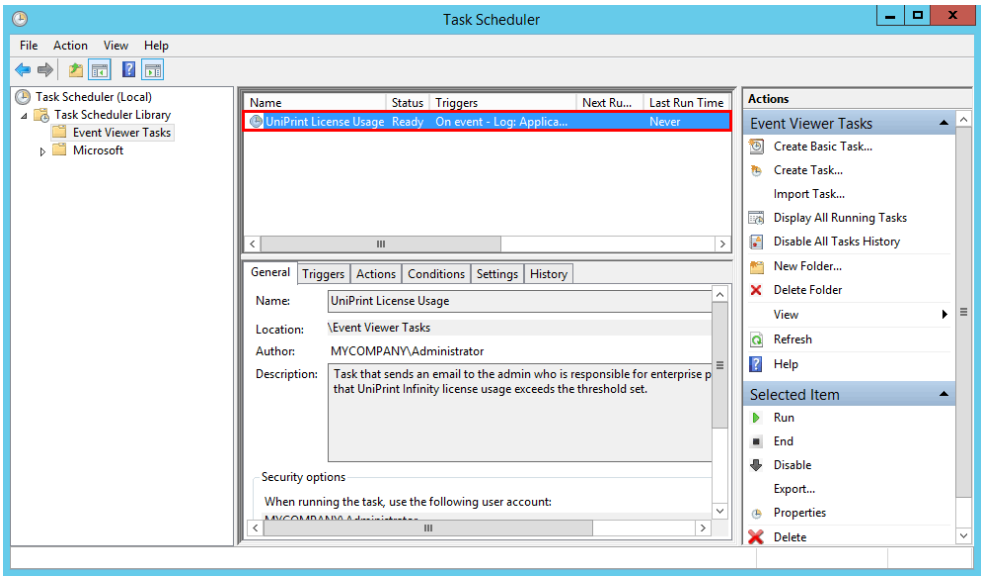
10. Ensure that **Start a program** is selected and then click **Next**.



11. Under **Program/script**, enter **`powershell.exe`**. Beside **Add argument (optional)**, enter the full path to the **SendUPEmail.ps1** script, for example, **`C:\Scripts\SendUPEmail.ps1`** and then click **Next**.



12. The task will appear in the **Event Viewer Tasks**.



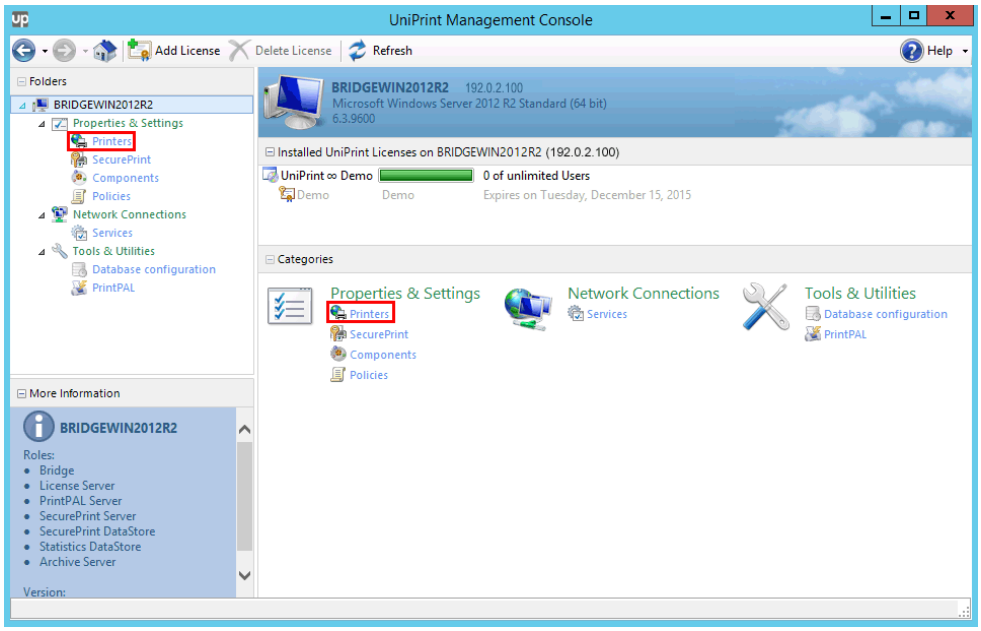
Searching For A Particular Printer

If the number of printers exceeds the space allotted on the screen, you may need to do a search or filter your printer list in order to configure them. The following instructions can also be applied to the UniPrint Print Server and UniPrint Application Server.

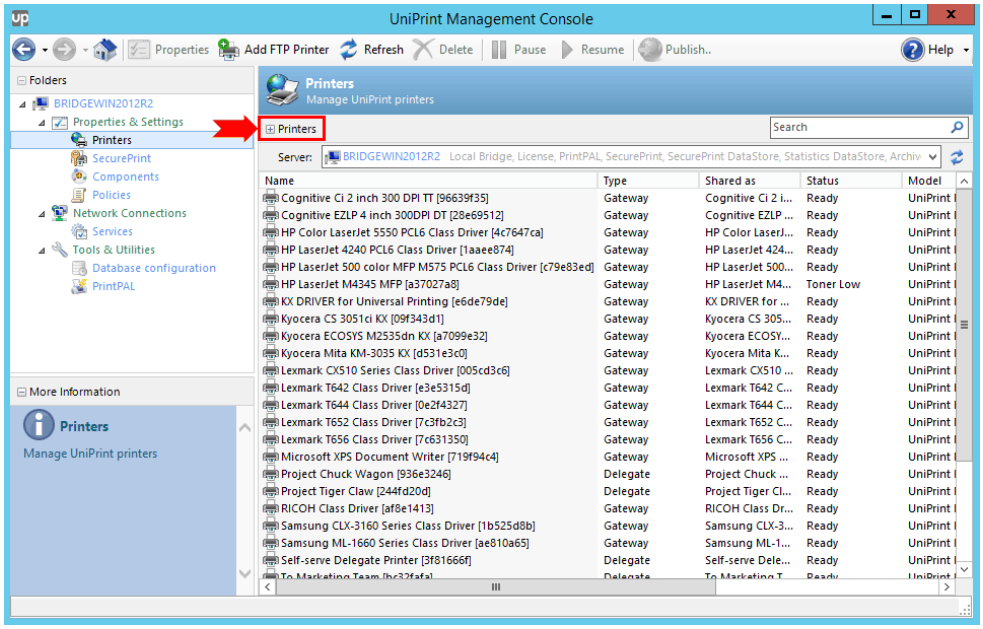
To search for a particular printer, do the following:

1. From any UniPrint component, open the **UniPrint Management Console**.

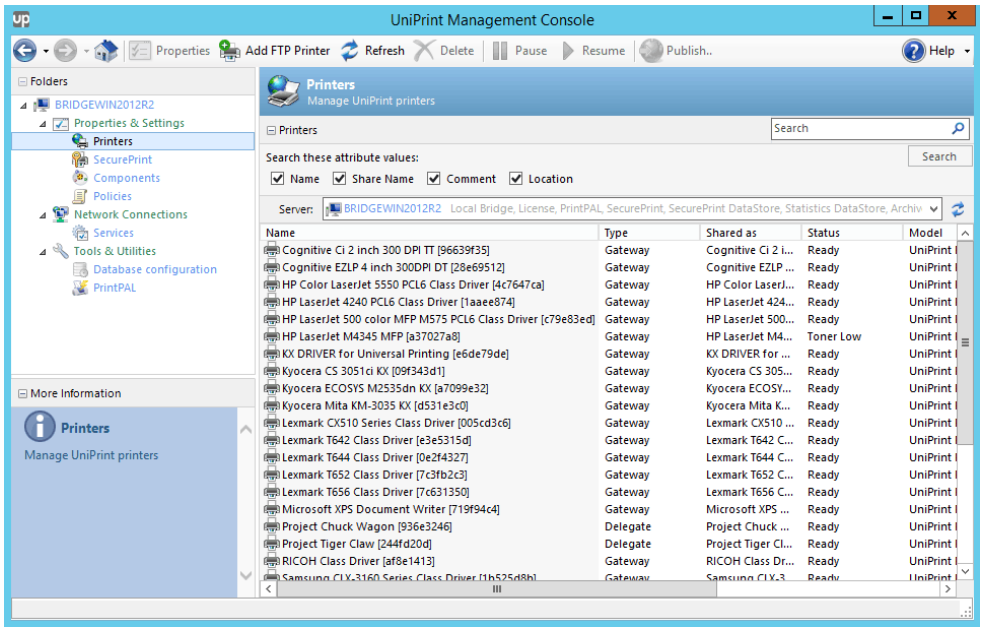
2. Under **Properties & Settings**, click **Printers**.



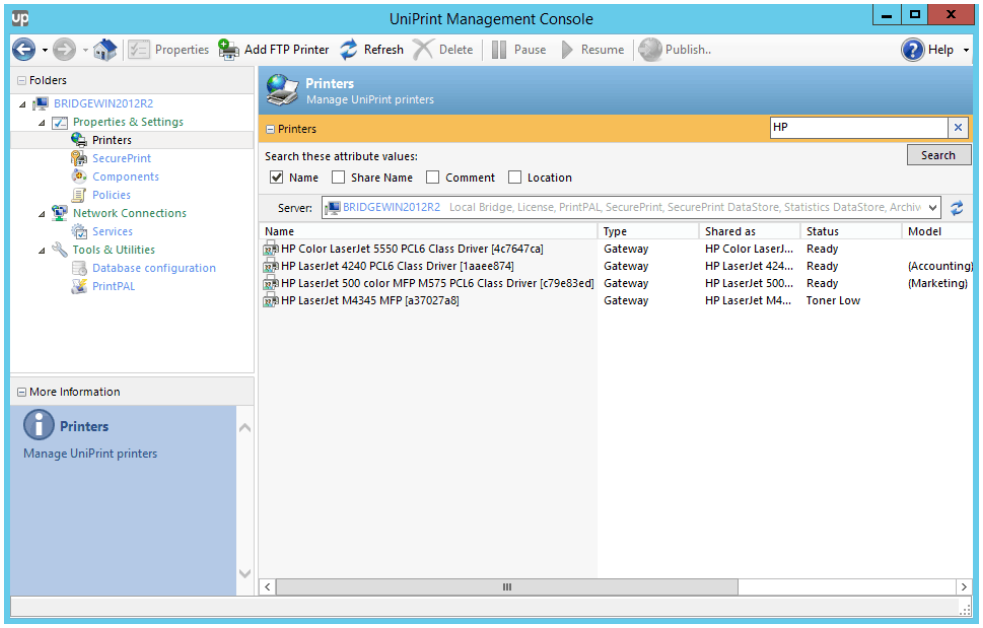
3. Click the plus sign beside **Printers**.



4. Select a filter attribute and then type in the **Search** box.



5. The printer list will be filtered as you type in the **Search** box and the printer bar will turn orange to indicate that a filter has been applied.



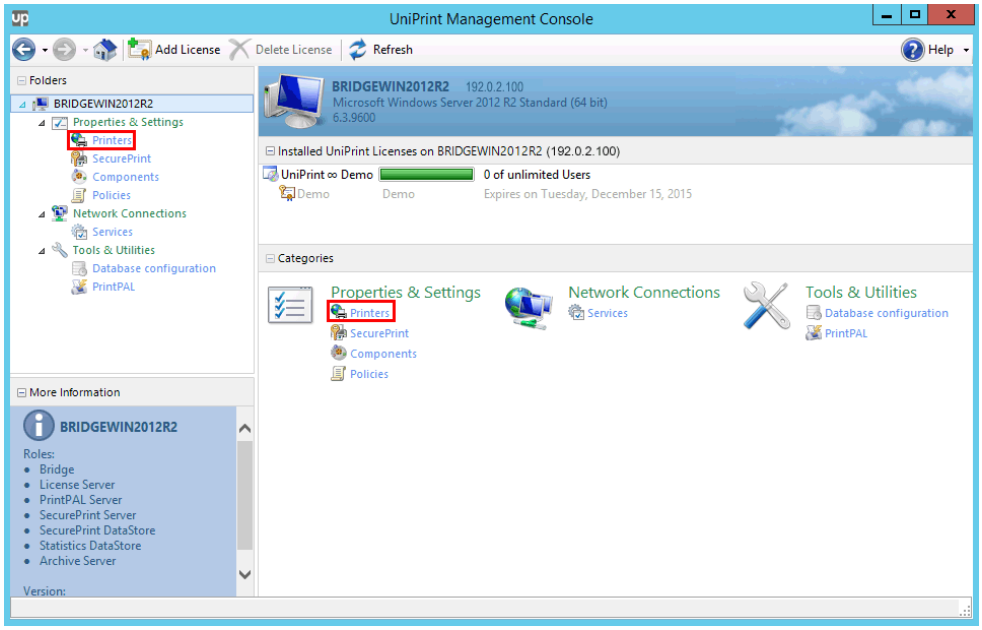
NOTE: To remove the filter, clear the **Search** box, select all filter attributes and then click **Refresh**.

Changing Default Printer Properties for Gateway Printers Globally For All Users

From the UniPrint Bridge, administrators can change the default printer preferences of a single or multiple Gateway printer(s) for all users.

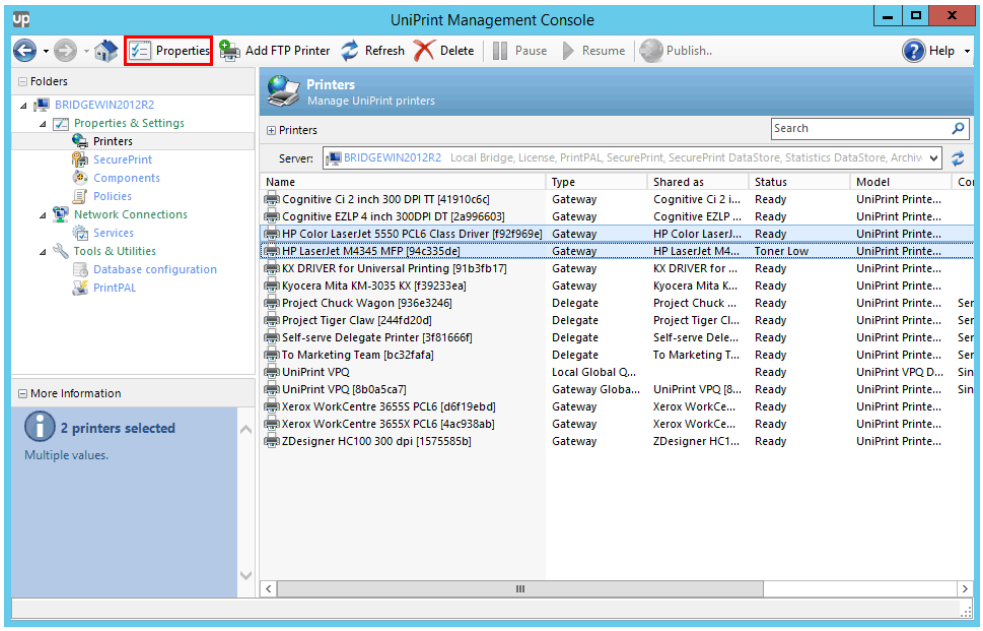
1. On the UniPrint Bridge, open the **UniPrint Management Console**.

2. Under **Properties & Settings**, click **Printers**.



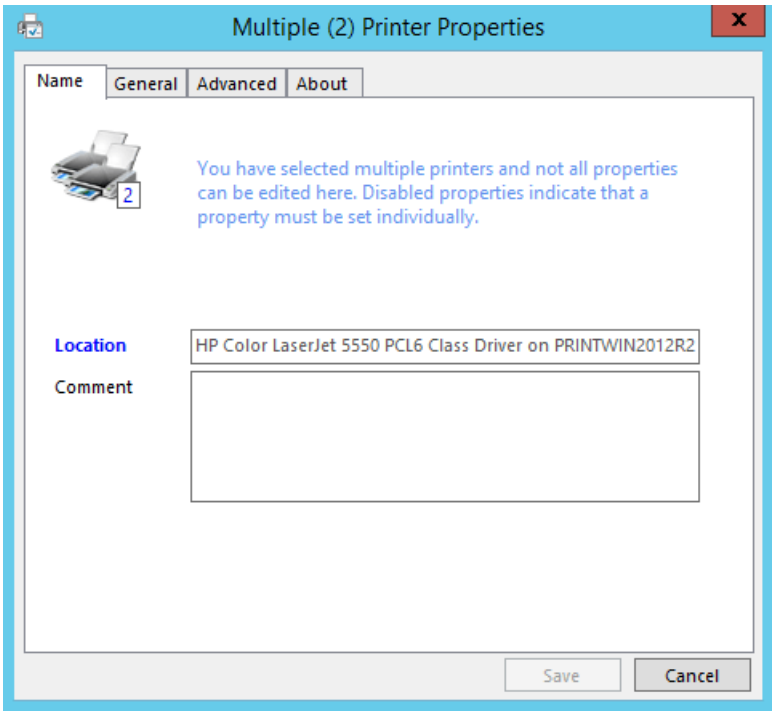
3. Click to select a printer or multiple printers from the details pane. Multiple printers can be selected by pressing **CTRL** and then clicking the desired printers.

4. Click **Properties**.



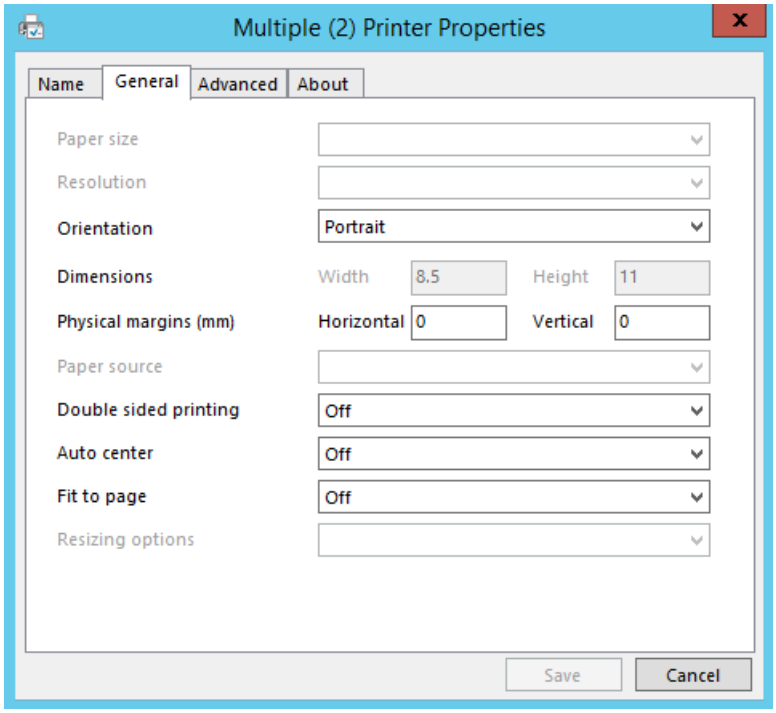
5. If multiple printers are selected, only the common properties are shown. Blank or disabled fields indicate that the properties are not the same and must be set individually. Changing a property will change it for all selected printers.

In the **Name** tab, only the comment can be changed.



NOTE: The name and shared name of a UniPrint Gateway printer can be changed by using Publish Options on the UniPrint Print Server and then republishing the printer to the UniPrint Bridge.

In the **General** tab, you can only set the active properties.



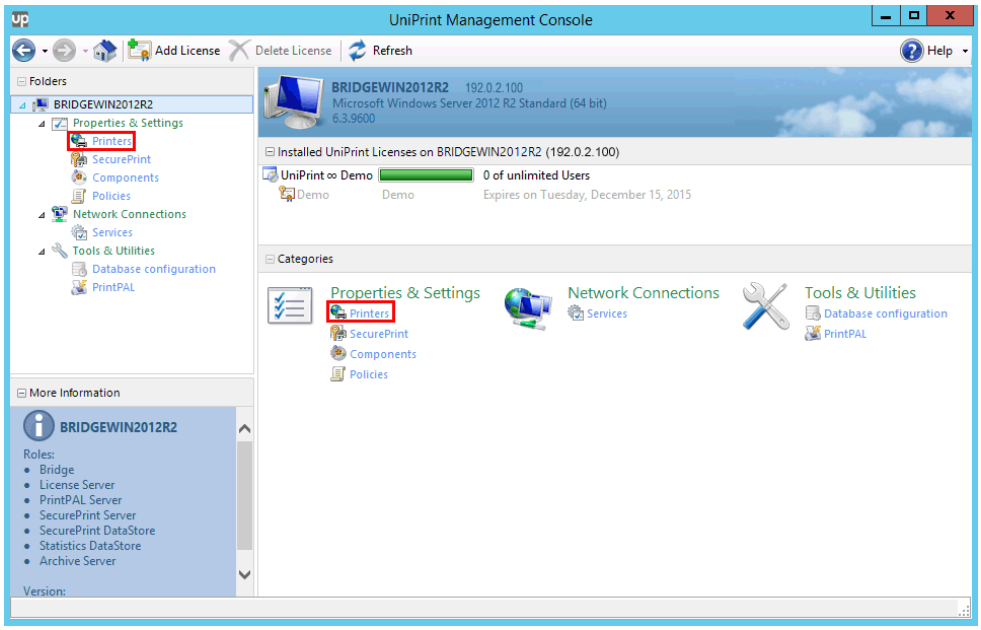
6. Change the desired properties and then click **Save**.

Adding a Lexmark/HP FTP Printer

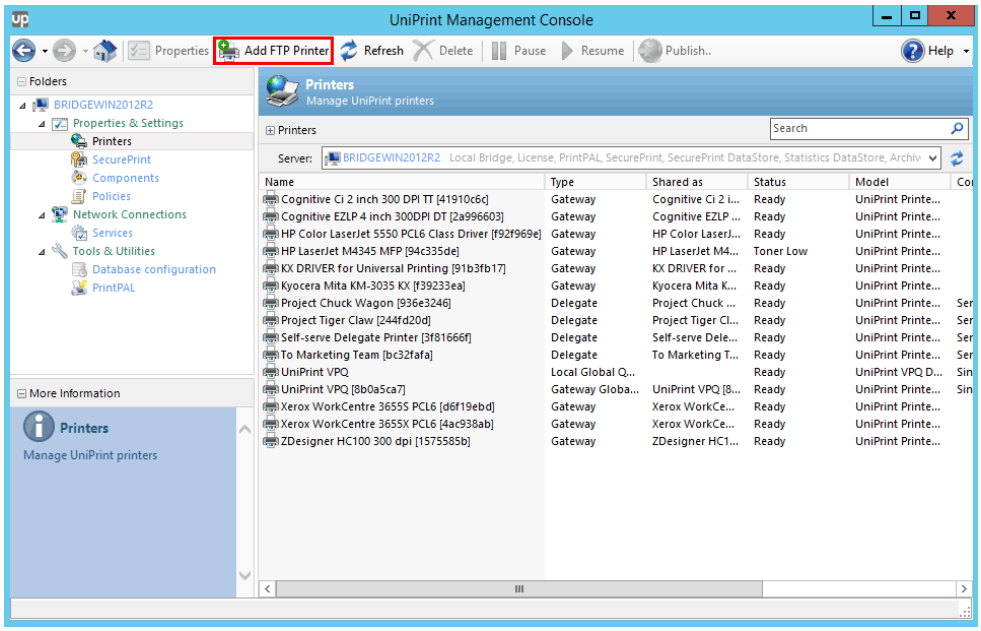
UniPrint Infinity can be defined and configured to send print jobs directly to Lexmark/HP FTP printers without going through a UniPrint Print Server. Since each UniPrint-ready Lexmark/HP FTP printer acts as its own print server, it can directly interpret PDF files without installing native printer drivers.

1. From the UniPrint Bridge, open the **UniPrint Management Console**.

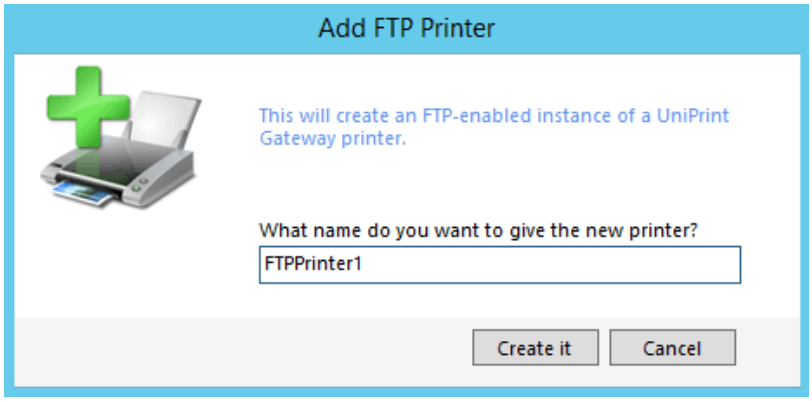
2. Under **Properties & Settings**, click **Printers**.



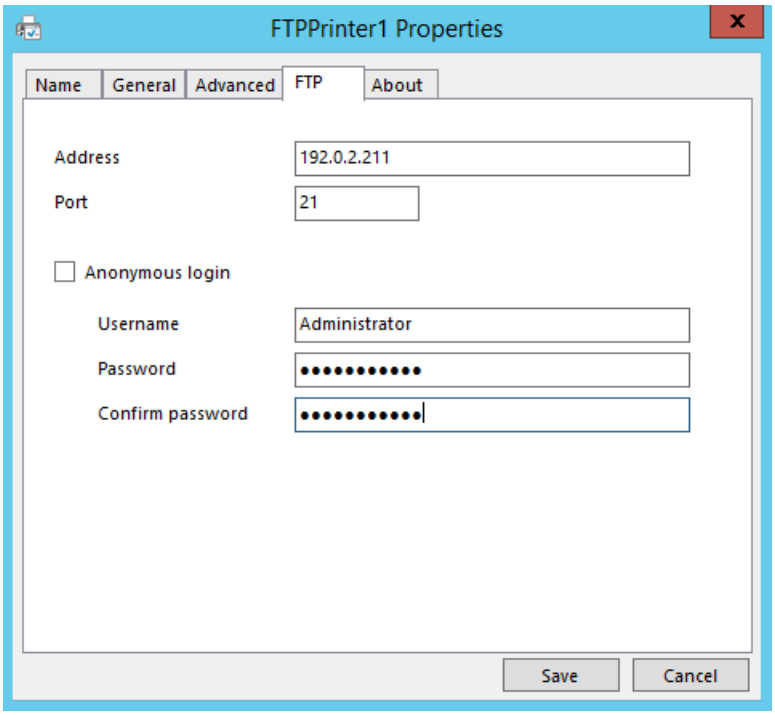
3. Click **Add FTP Printers**.



4. Enter the new printer name, then click **Create it**.

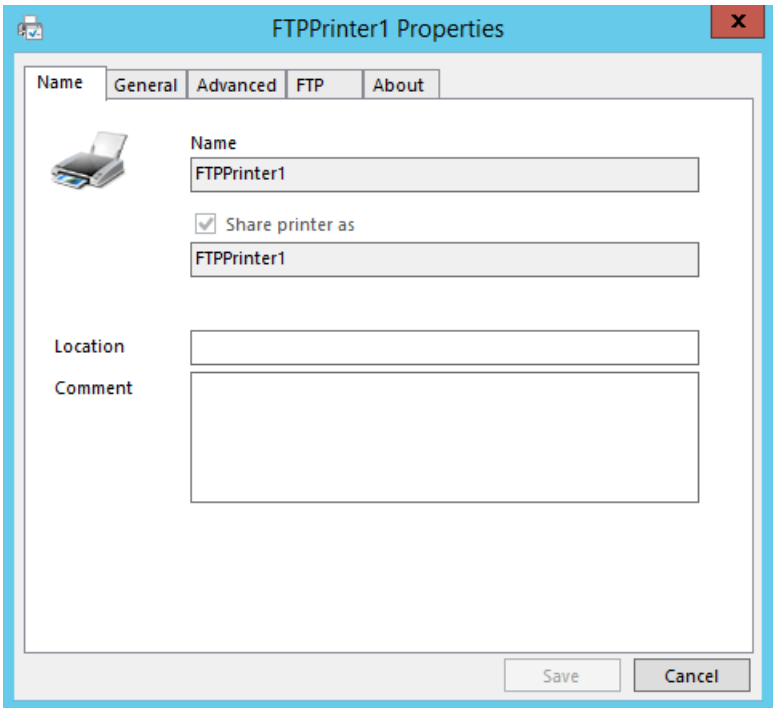


5. In **FTP** tab, enter the information that is relevant to your configuration.

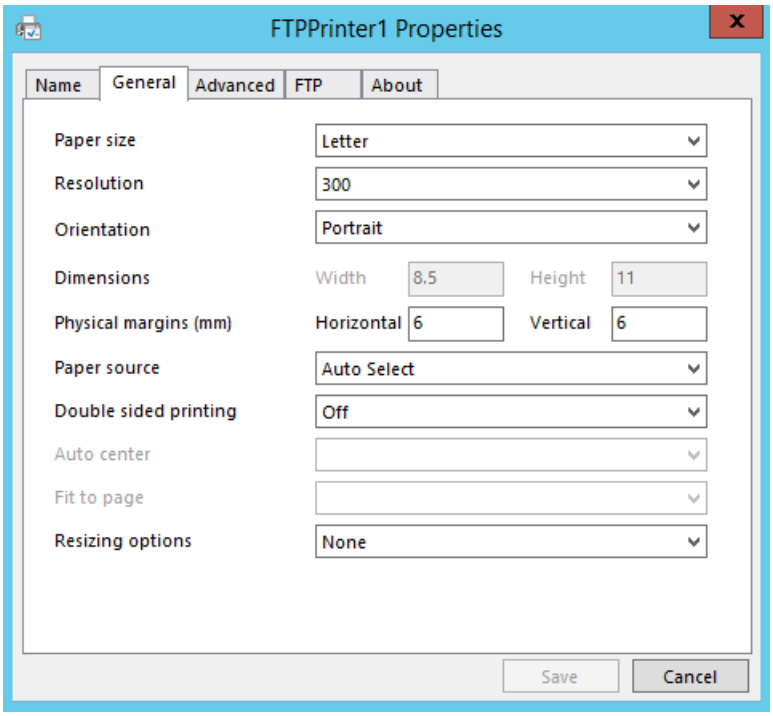


- **Address**: The IP address of the Lexmark/HP FTP printer.
- **Port**: The FTP listener port of the Lexmark/HP FTP printer. *Default is 21.*
- **Anonymous Login**: Click to select if anonymous logins are allowed. If this check box is cleared enter the Username, Password and Confirm Password.
- **Username**: The FTP account for submitting print jobs to the Lexmark/HP FTP printer.
- **Password**: The FTP account password for submitting print jobs to the Lexmark/HP FTP printer.
- **Confirm Password**: Enter the FTP account password again.

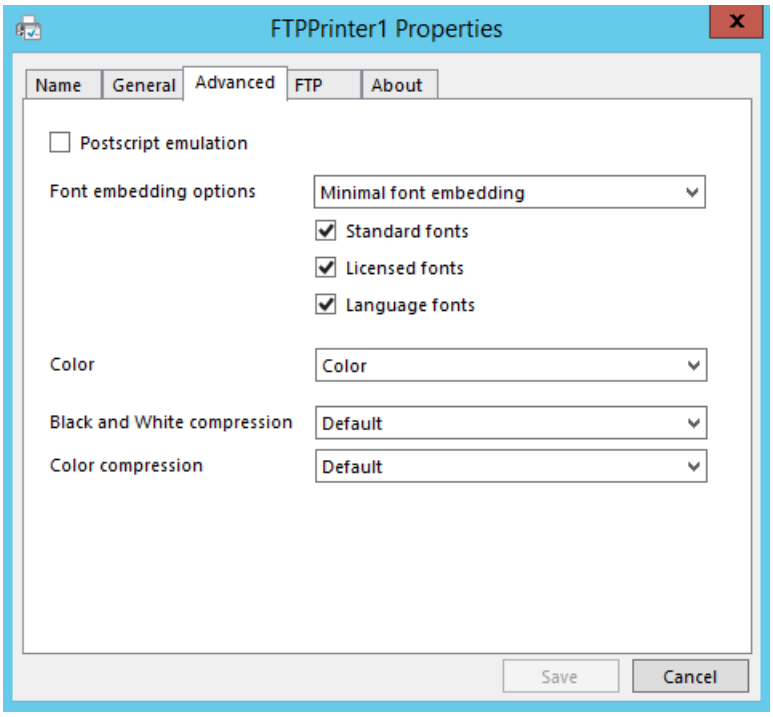
6. In the **Name** tab, enter the **Location** and **Comment** for the Lexmark/HP FTP printer.



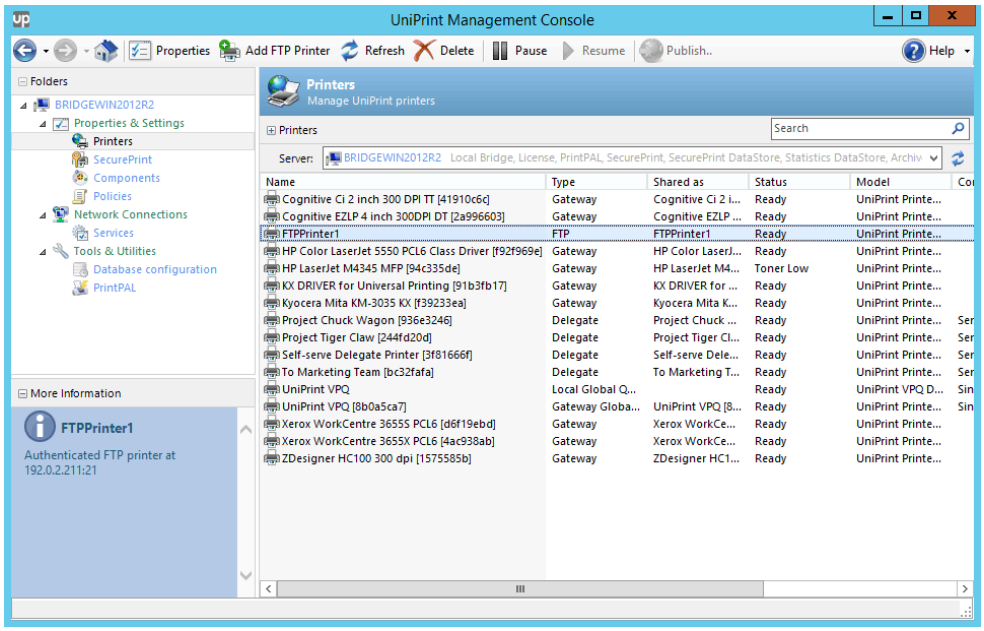
7. Click the **General** tab to edit the default printer properties as desired.



8. Click the **Advanced** tab to edit the default settings as desired.



9. Click **Save**. The new printer should appear in the printer list as type **FTP**.

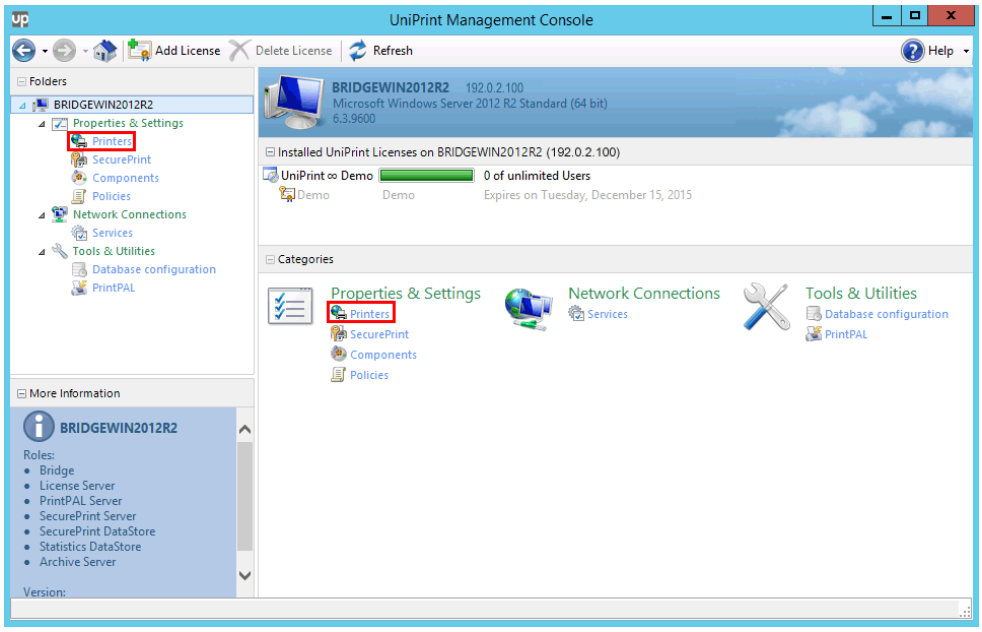


Deleting a Gateway Printer from the UniPrint Bridge

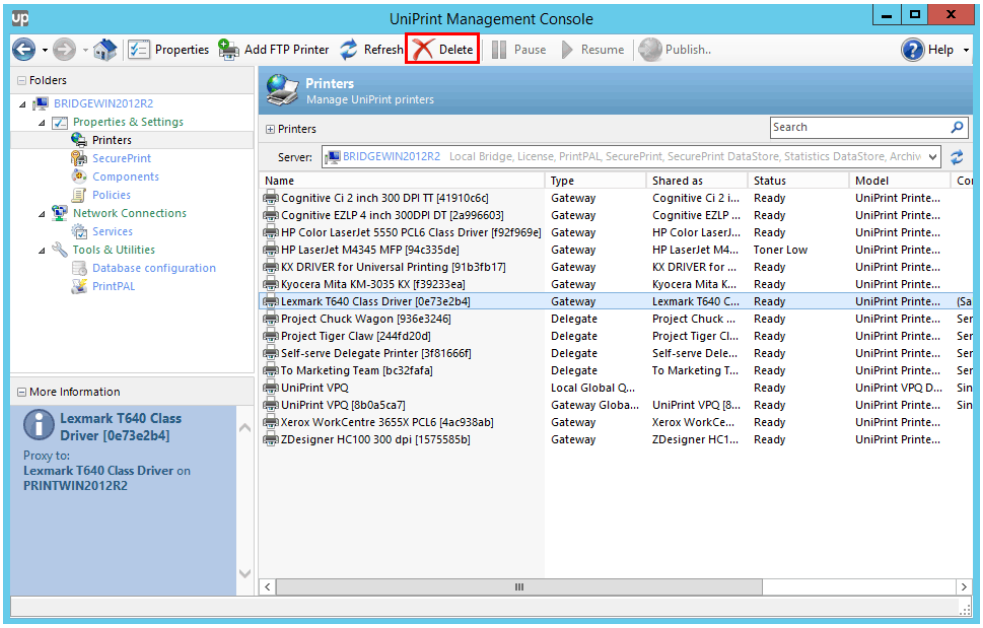
Deleting a printer from the UniPrint Bridge does not delete it from the UniPrint Print Server.

1. From the UniPrint Bridge, open the **UniPrint Management Console**.

2. Under **Properties & Settings**, click **Printers**.



3. Click to select the printer that you want to delete and then click **Delete**.



4. Click **Yes** to confirm that you want to delete the selected printer.

To recreate the printer later, click **Publish** on the UniPrint Print Server's **Printers** screen.

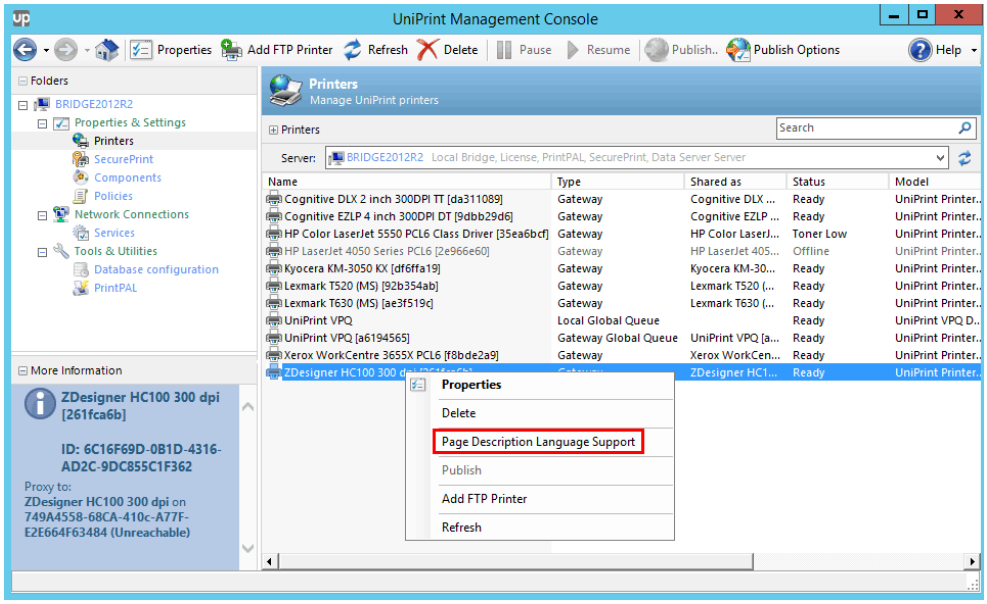
Enabling PDL Support for Label Printers

Page Description Language (PDL) support was primarily designed to support label makers, for example, Zebra printers that use ZPL and ZPL II. It allows ASCII text characters to be sent directly to the printer without creating a PDF.

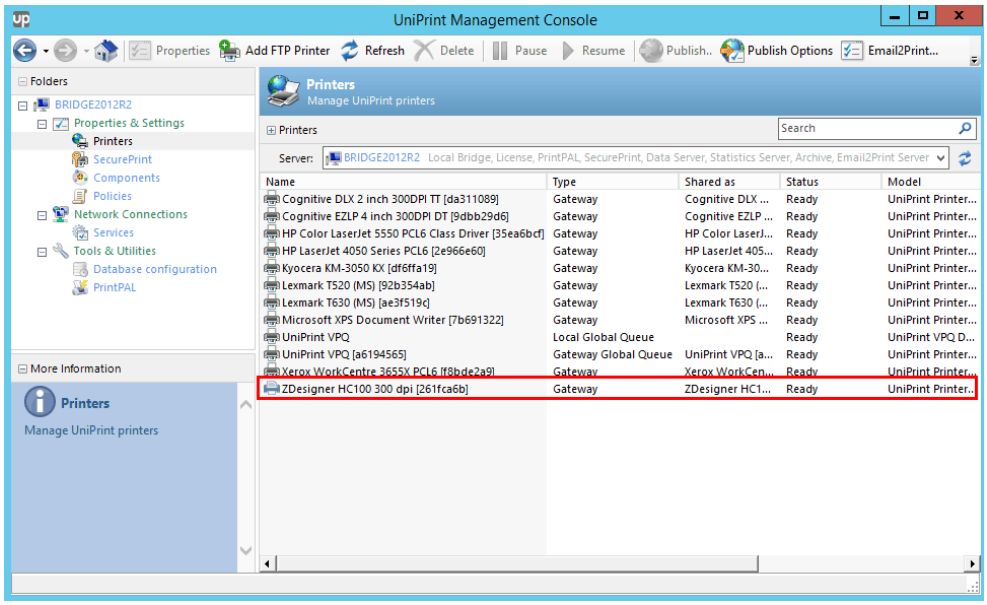
To enable PDL support, do the following:

1. On the UniPrint Bridge, under **Properties & Settings**, click **Printers**.

2. Right-click a label printer and then select **Page Description Language Support**.



3. The printer icon will change from to indicating that PDL support has been enabled for this printer.



NOTE: If a Zebra printer is selected, the default paper for the print job will automatically be set to the custom Zebra label size. If a different label printer is desired (not a Zebra), the user must exit the printer selection dialog box entirely, in order to reset the default paper size to the original default size.

Configuring UniPrint Print Server

From the UniPrint Print Server, administrators can add new Gateway printers, publish them to the UniPrint Bridge, specify how printers are published, and create custom printer profiles.

Adding a Gateway printer

To add a Gateway printer on the UniPrint Print Server, do the following:

1. On the UniPrint Print Server, click **Start** and then click the **Control Panel** tile.

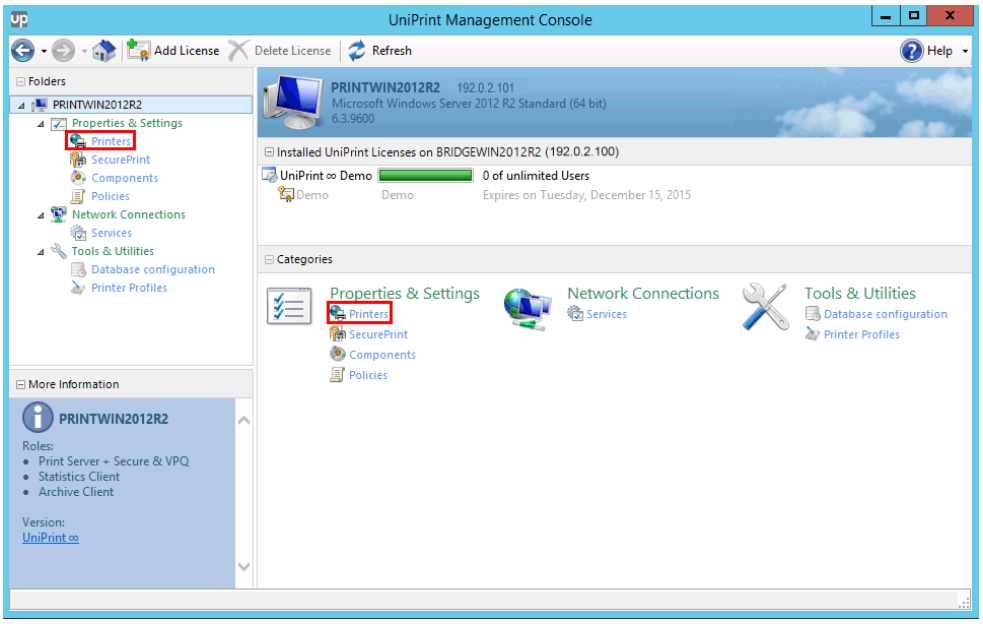
2. Click **Devices and Printers**.

3. Click **Add a printer** and then follow the printer manufacturer's instructions for installing their printer driver.

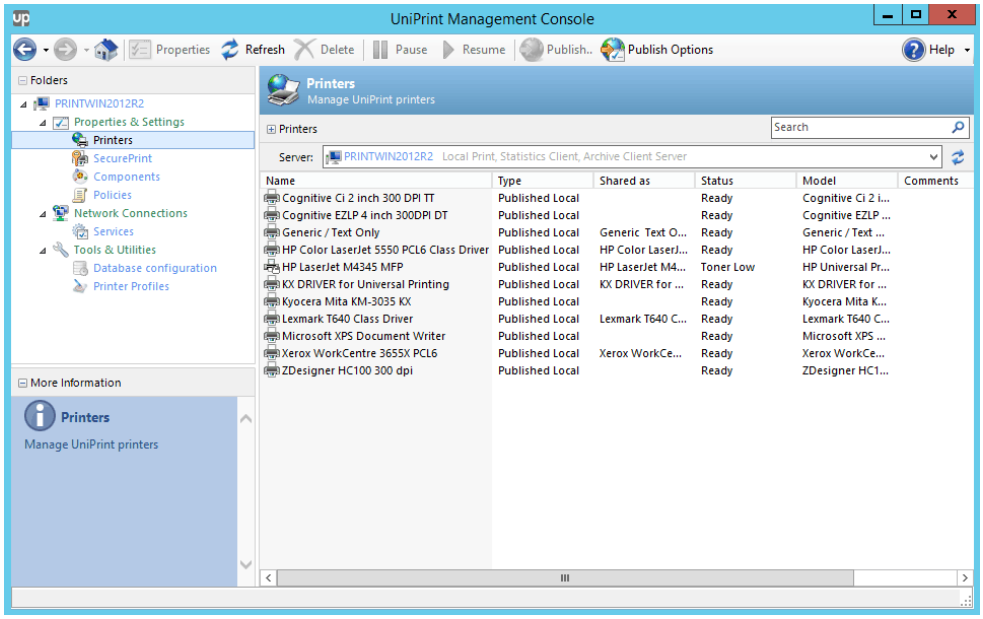
NOTE: It is recommended that PostScript print drivers be installed over PCL and universal print drivers to achieve optimal UniPrint performance.

4. Open the **UniPrint Management Console**.

5. Under **Properties & Settings**, click **Printers**.

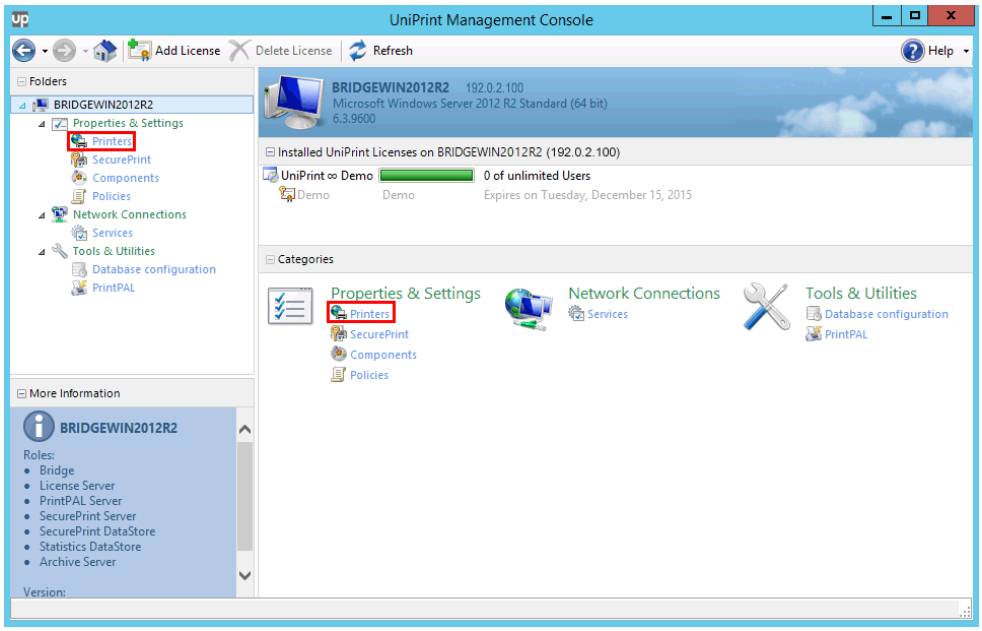


6. Ensure that the test printer appears of type **Published Local**.

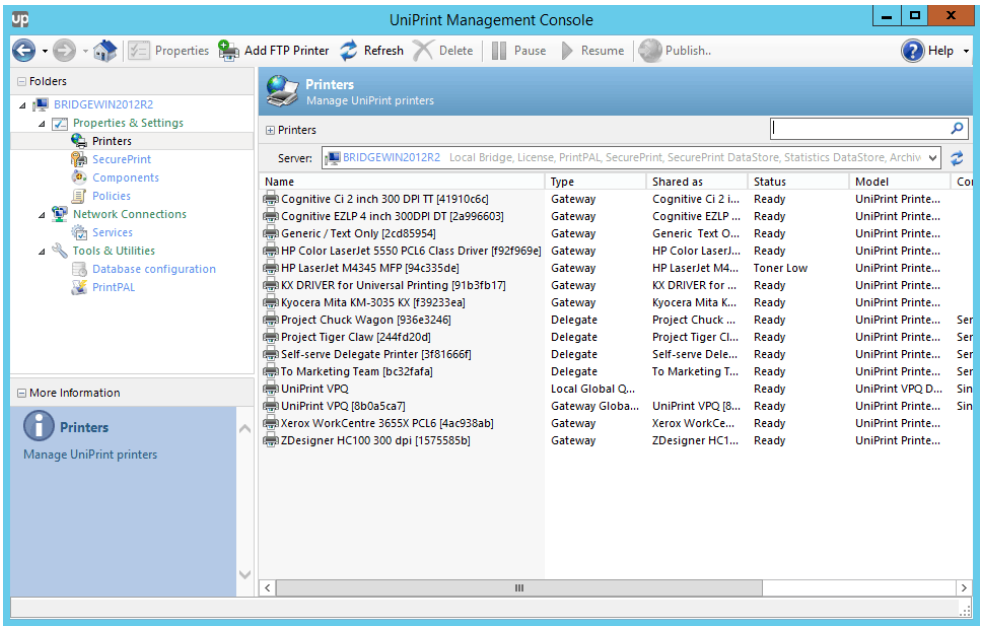


7. On the UniPrint Bridge, open the **UniPrint Management Console**.

8. Under **Properties & Settings**, click **Printers**.



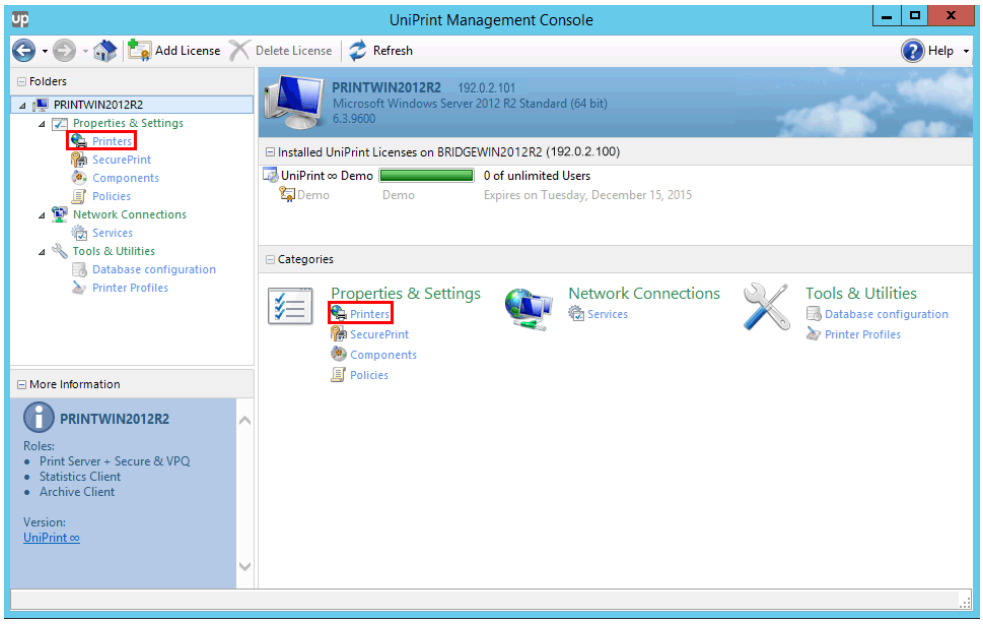
9. The new printer will appear in the printer list of type **Gateway.**



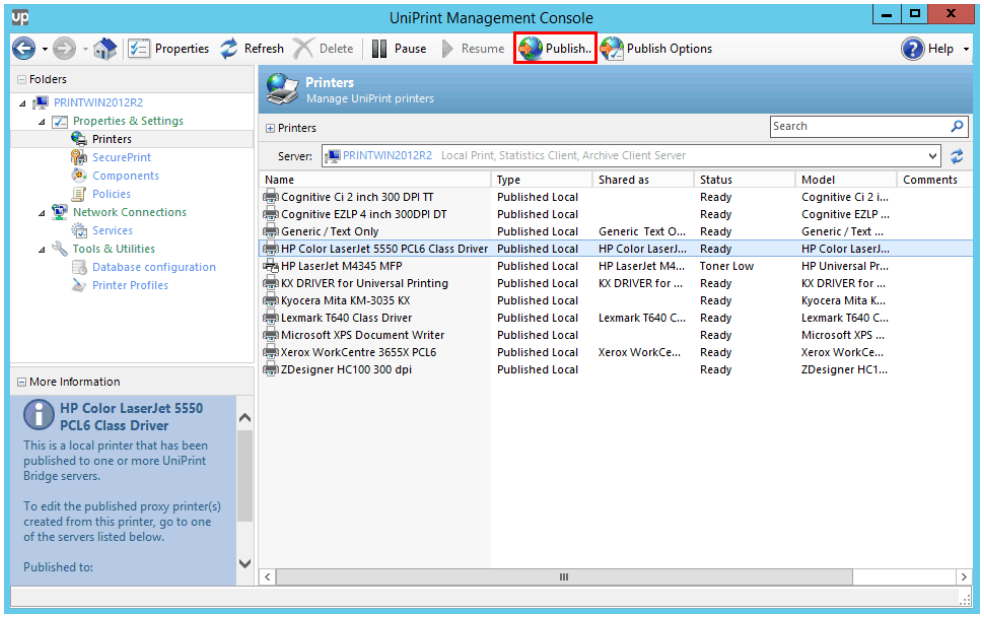
Re-publishing a Printer to the UniPrint Bridge

1. On the UniPrint Print Server, open the **UniPrint Management Console**.

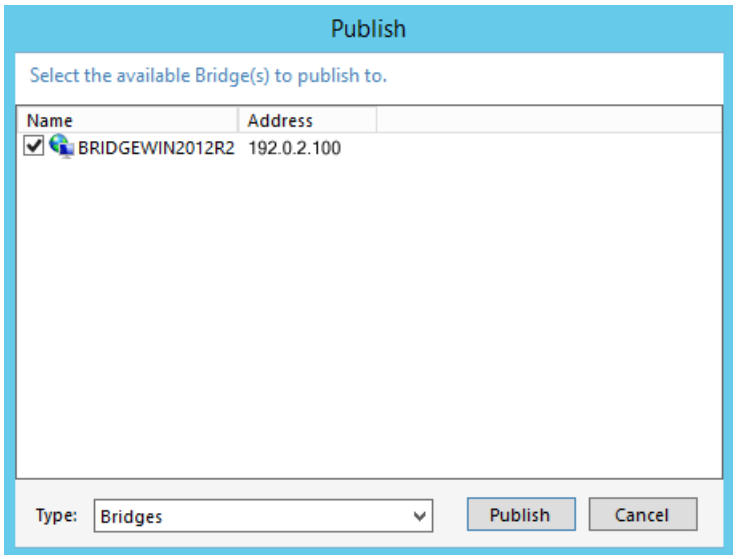
2. Under **Properties & Settings**, click **Printers**.



3. Click to select a printer to re-publish and then click **Publish**.

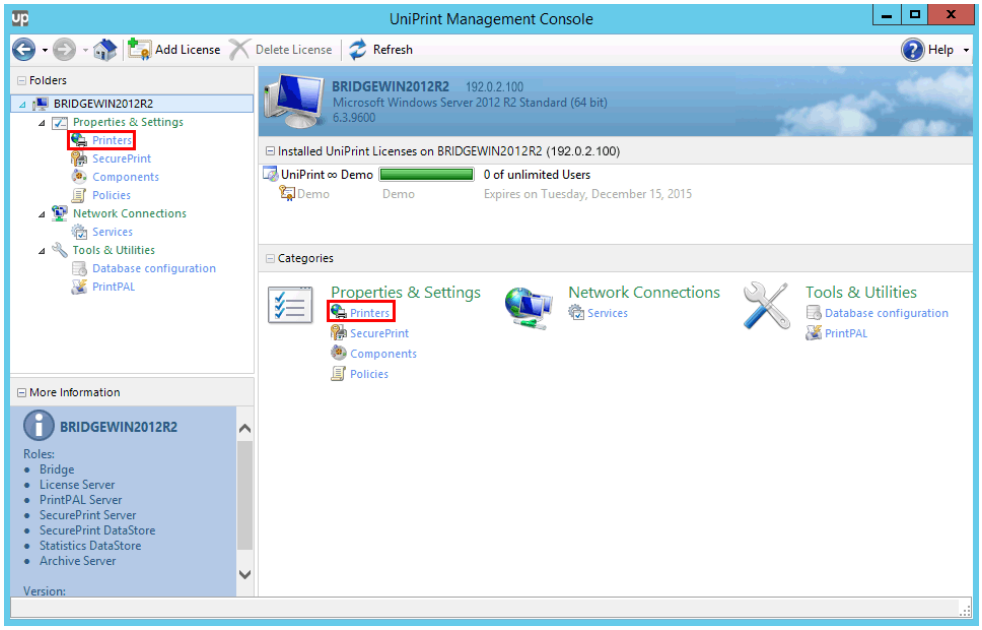


4. Select the UniPrint Bridge(s) to which you want to publish the printer and then click **Publish**.



5. On the UniPrint Bridge, open the **UniPrint Management Console**.

6. Under **Properties & Settings**, click **Printers**.



7. Click **Refresh,** if the printer does not immediately appear.

8. If the printer still does not appear, restart the UniPrint Control Service. Under **Network Connections**, click **Services**. Click to select **UniPrint Control Service** and then click .

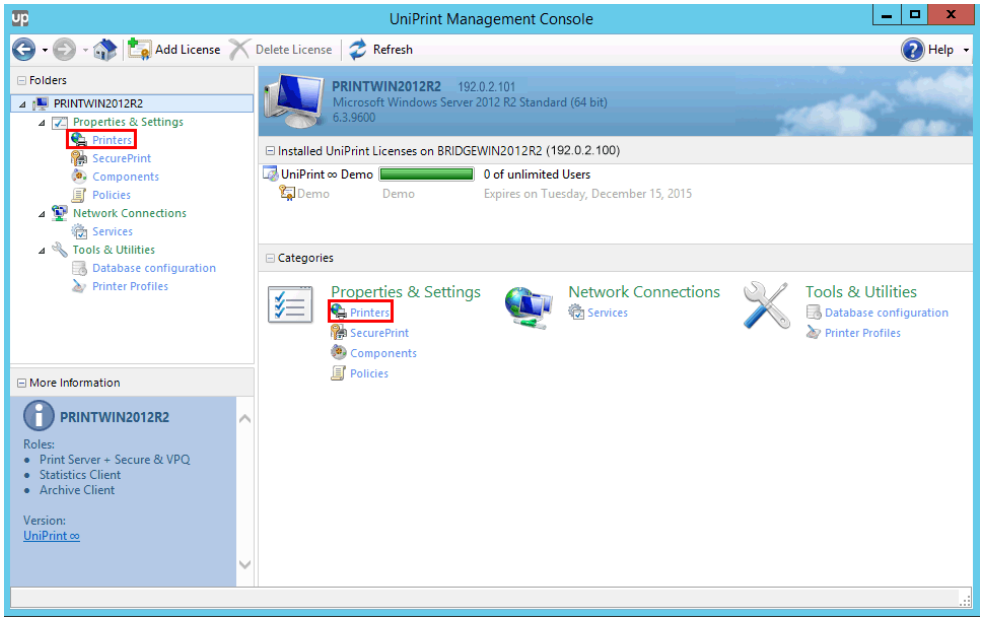
Changing How Gateway Printers are Published to the UniPrint Bridge

Part of the UniPrint Print Server's function is to enumerate available printers on each print server and make them available on the UniPrint Bridge. If a printer is inadvertently deleted from the UniPrint Bridge, the UniPrint Print Server can republish the printer to the UniPrint Bridge.

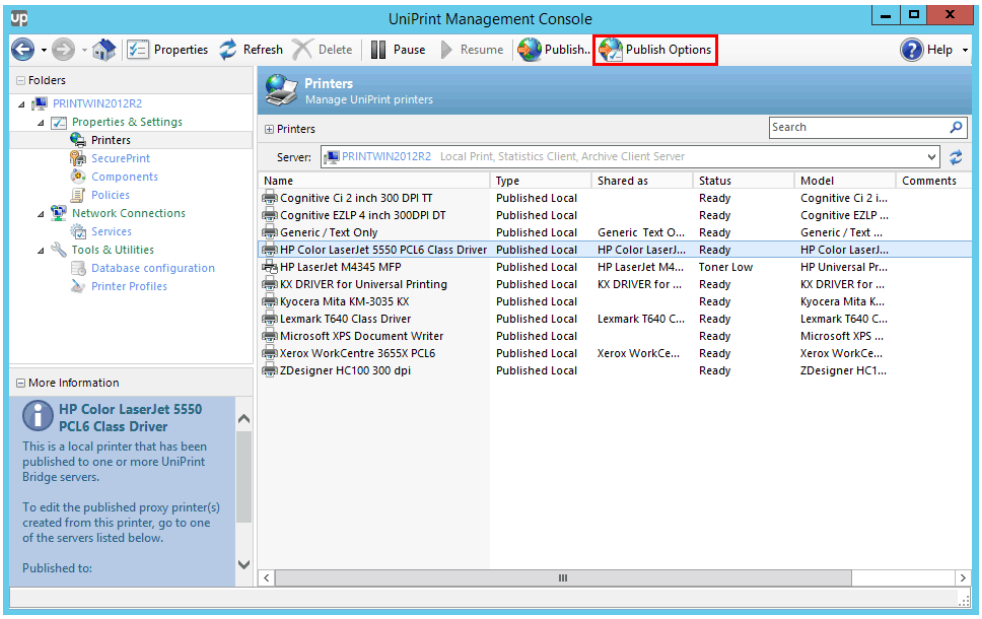
To change how printers are published to the UniPrint Bridge, do the following:

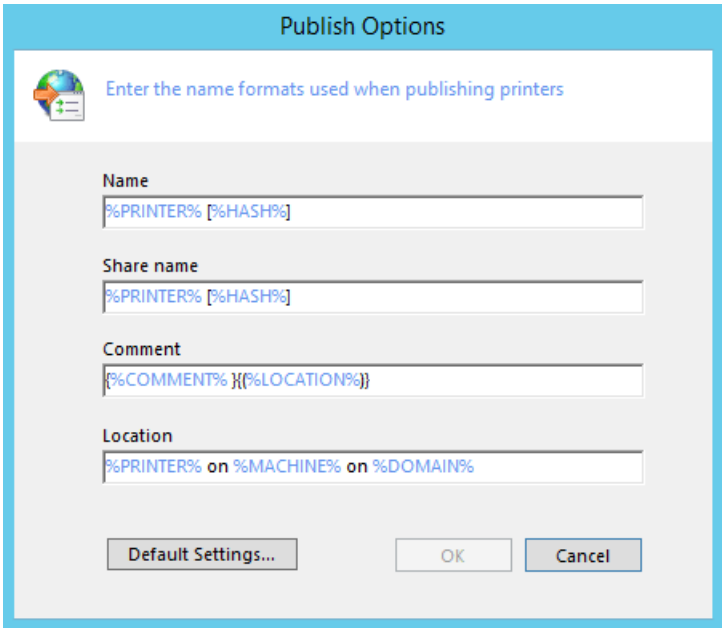
1. On the UniPrint Print Server, open the **UniPrint Management Console**.

2. Under **Properties & Settings**, click **Printers**.



3. Click to select a printer and then click **Publish Options**.



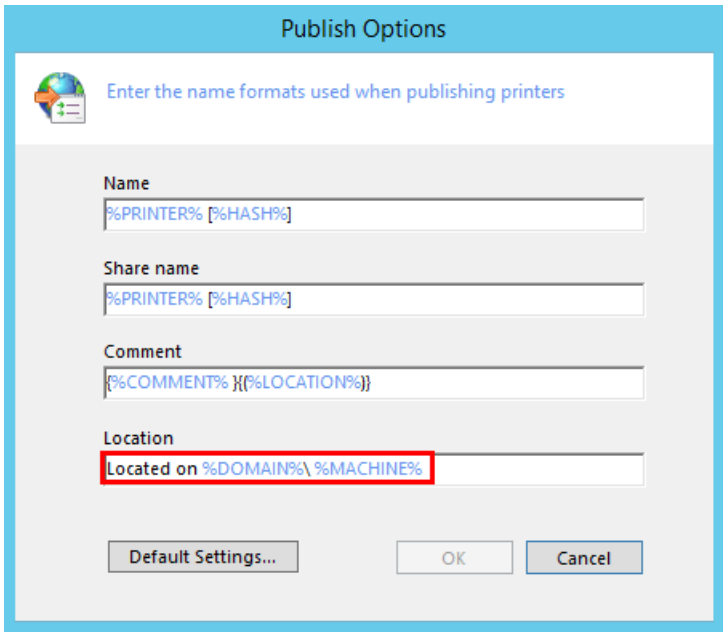


Placeholders are used to represent variables and can be rearranged or deleted depending on how you would like the printers to be published and displayed on the UniPrint Bridge.

%PRINTER%	Printer name.
%HASH%	Hash number assigned by UniPrint to ensure each Gateway printer is unique.

%COMMENT%	Comments provide general information about the printer. UniPrint imports this information from the Comment field of the local Print Server queue.
%LOCATION%	Location describes where the printer is situated. UniPrint imports this information from the Location field of the local Print Server queue.
%MACHINE%	Print server name.
%DOMAIN%	Domain name of the print server.

4. Edit how you would like your printers to be published and then click **OK**. When published to the UniPrint Bridge the printer will appear as instructed through the **Publish Options** dialog box. Any previously published printers will remain unchanged.



NOTE: Adding a hash number to the printer name ensures distinctiveness between printers on the UniPrint Bridge. For example, if two printers with identical printer names are published from two different UniPrint Print Servers to the same UniPrint Bridge, then only one printer will be successfully added to the UniPrint Bridge.

5. Re-publish the printer to the UniPrint Bridge.

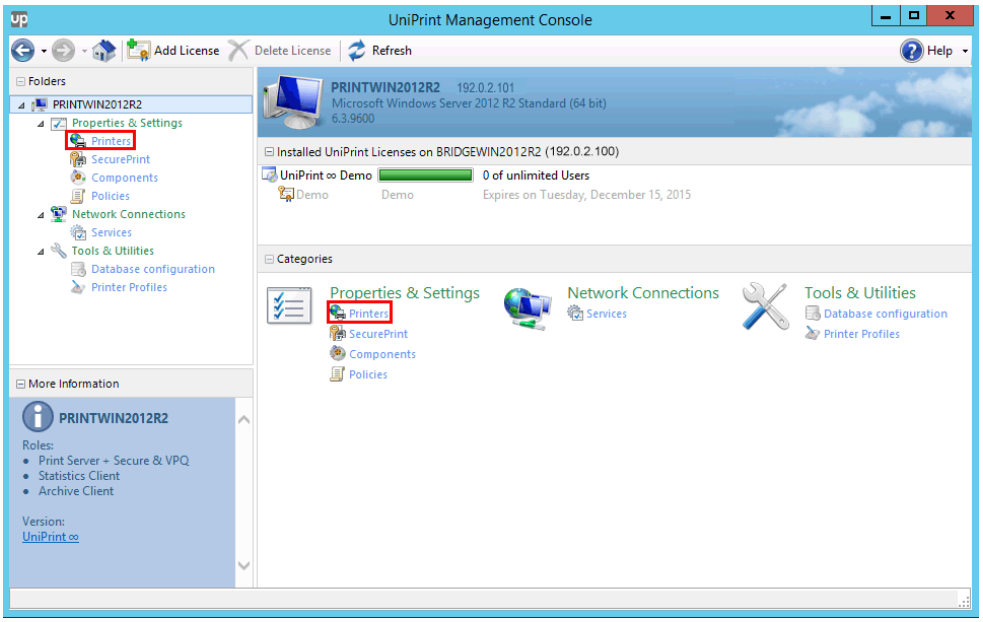
Setting Default Printer Properties for New & Republished Gateway Queues

Extended default printer properties can be set for newly created and republished Gateway printers. After setting default printer properties, any Gateway queue that is created or if a current Gateway printer is republished, will have these default printer properties applied. Printer properties for existing Gateway printers will remain affected until they are republished.

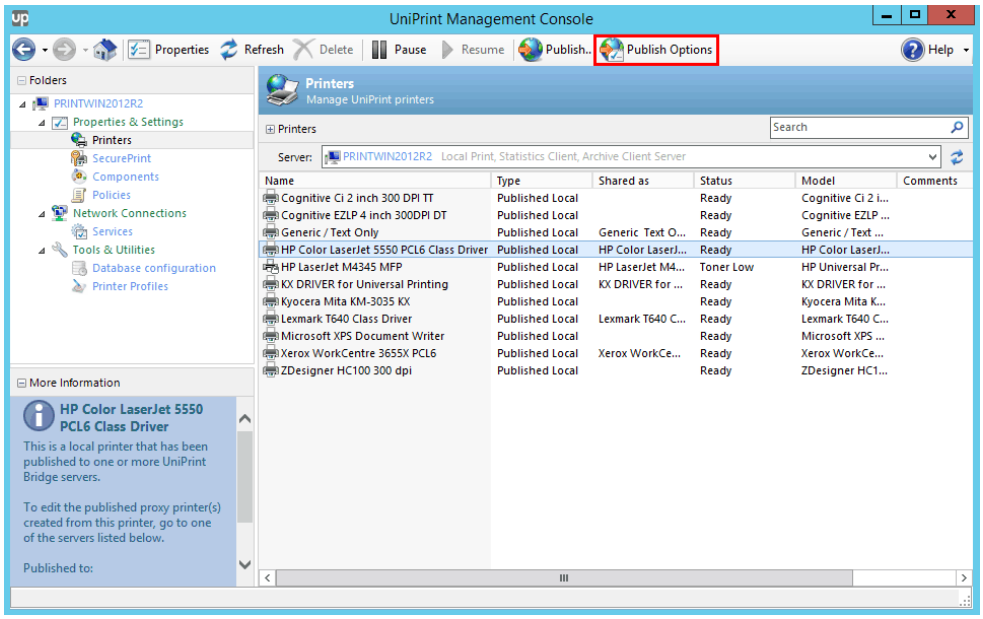
To set default Gateway printer properties, do the following:

1. On the UniPrint Print Server, open the **UniPrint Management Console**.

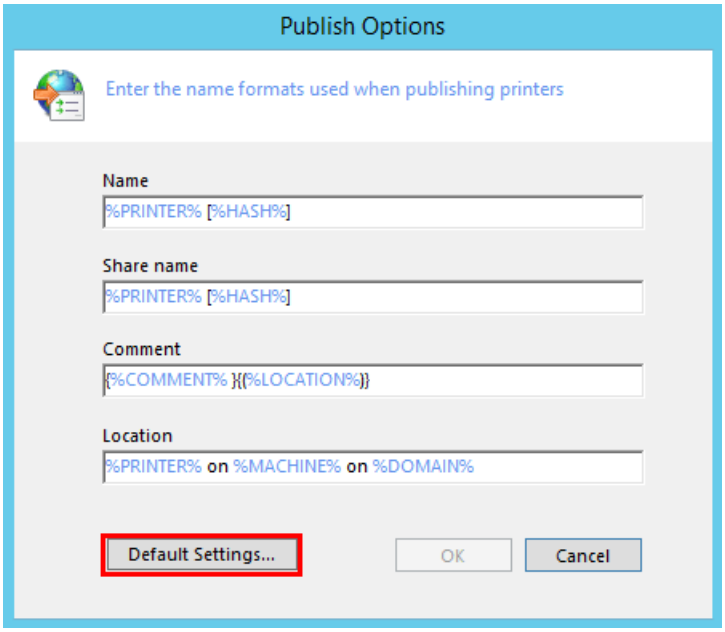
2. Under **Properties & Settings**, click **Printers**.



3. Click **Publish Options**.

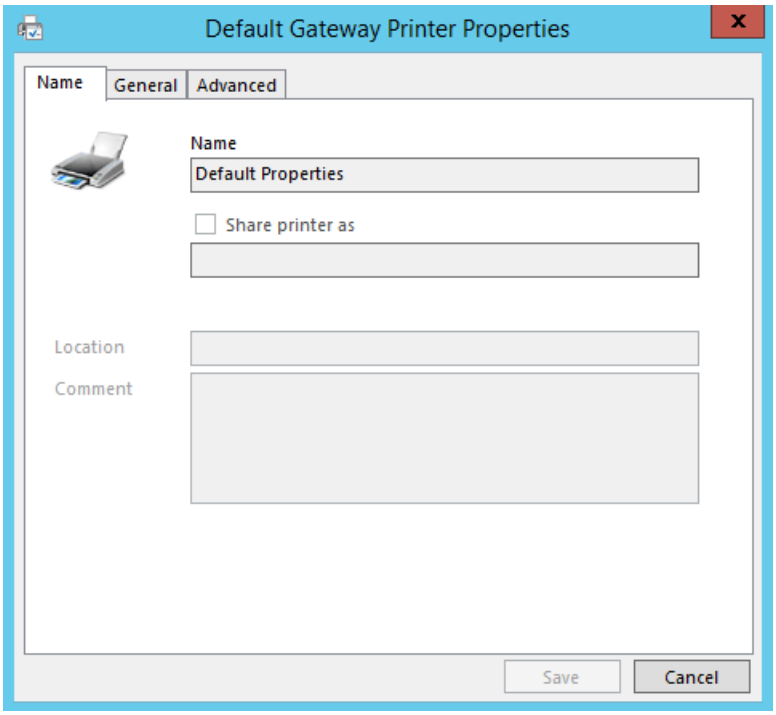


4. Click **Default Settings**.

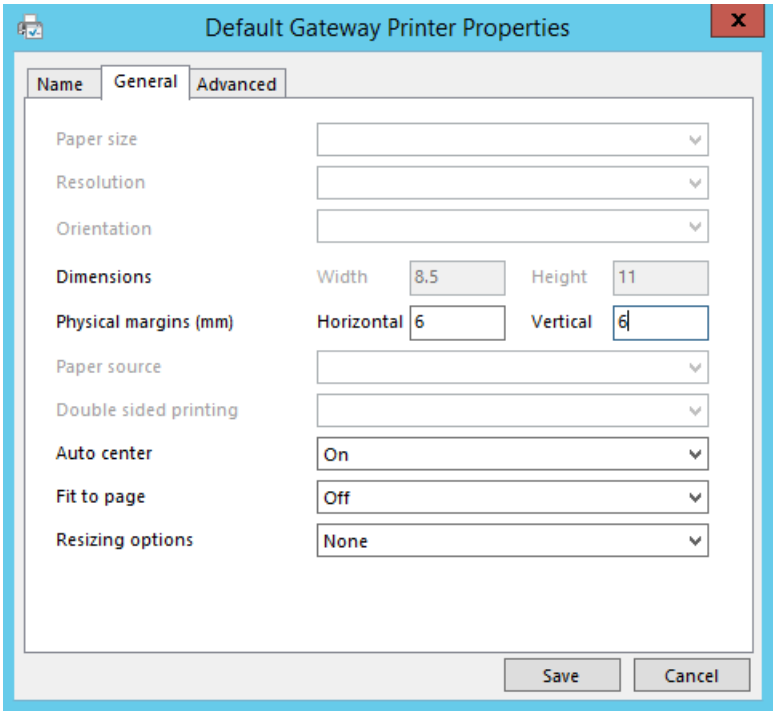


5. Enter administrative credentials for the UniPrint Bridge and then click **OK**.

6. Click the **General** or **Advanced** tab.



7. Change the desired properties and then click **Save**.

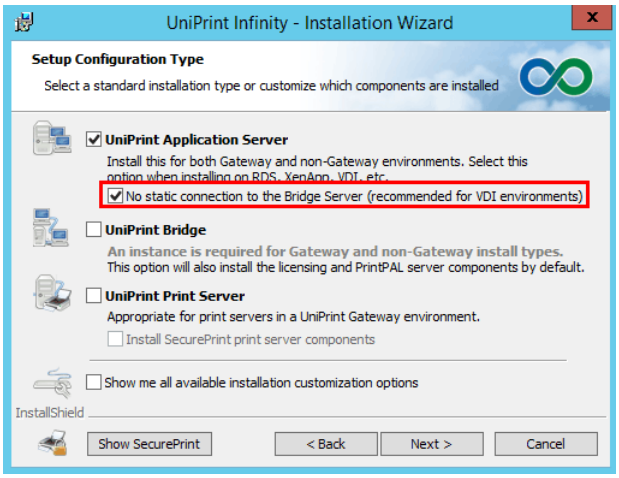


8. Click **Cancel** to exit **Publish Options**.

Enabling Font Replication

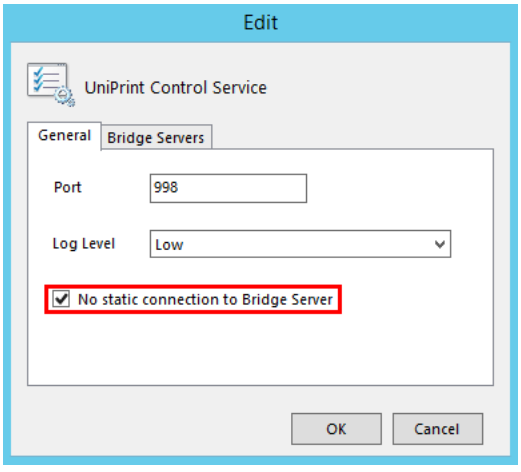
Daily at a pre-scheduled time, UniPrint queries all UniPrint Application Servers for newly installed fonts and replicates them to all UniPrint Print Servers. After fonts are replicated, font embedding is no longer required resulting in smaller print job file sizes, improved overall print job quality and reduced bandwidth consumption.

NOTE: Font replication will not function properly if **No static connection to Bridge Server** was selected during the UniPirnt Application Server installation.



To disable this option, do the following:

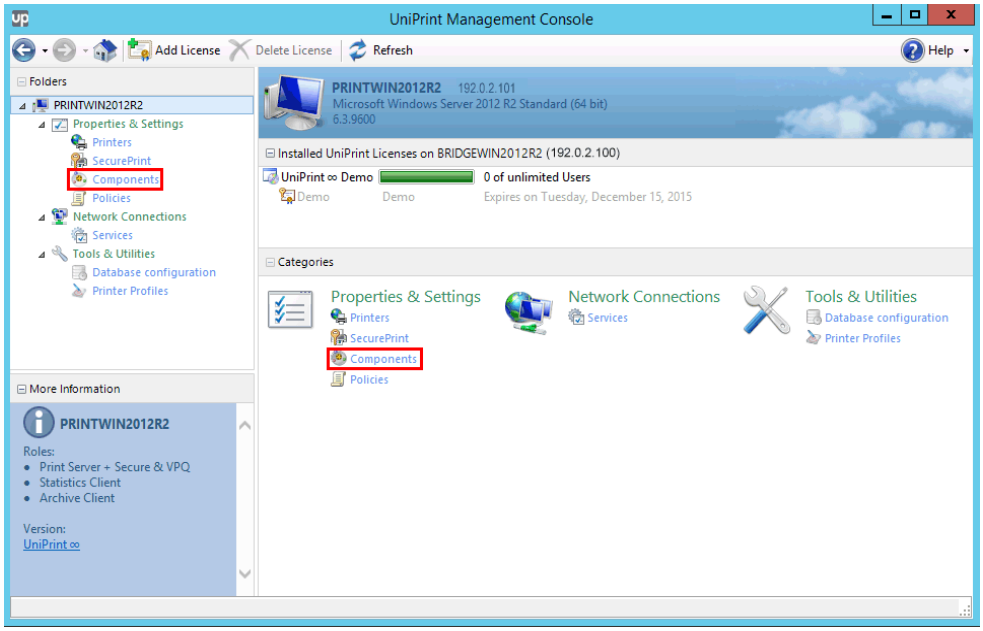
1. On the **Application Server**, open the **UniPrint Management Console**.
2. Under **Network Connections**, click **Services**
3. Right-click **UniPrint Control Service** and then select **Properties**.
4. In the **General** tab, clear **No static connection to Bridge Server** and then click **OK**.



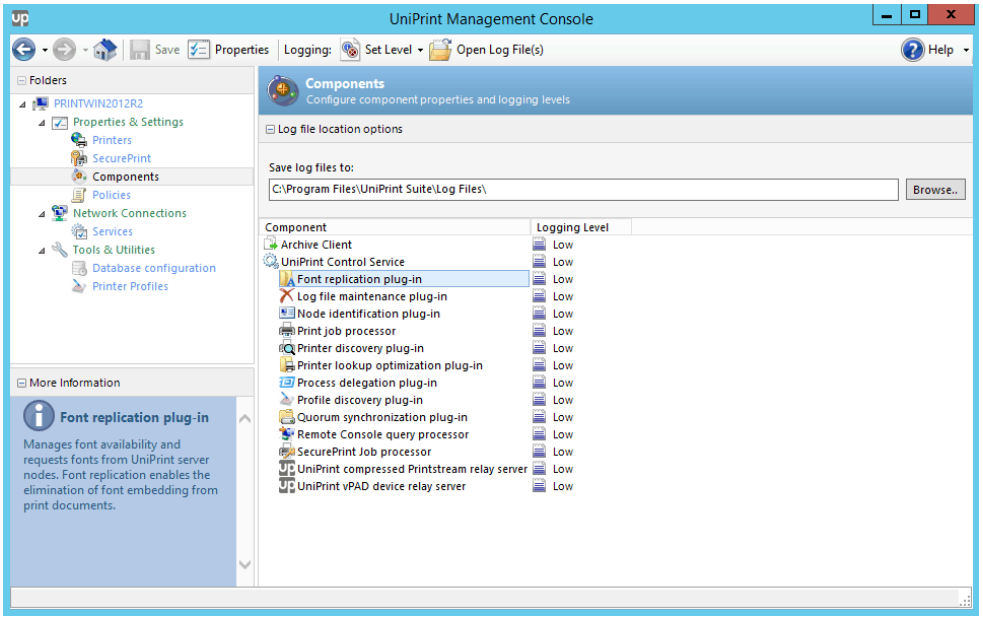
To enable font replication, do the following:

1. On the UniPrint Print Server, open the **UniPrint Management Console**.

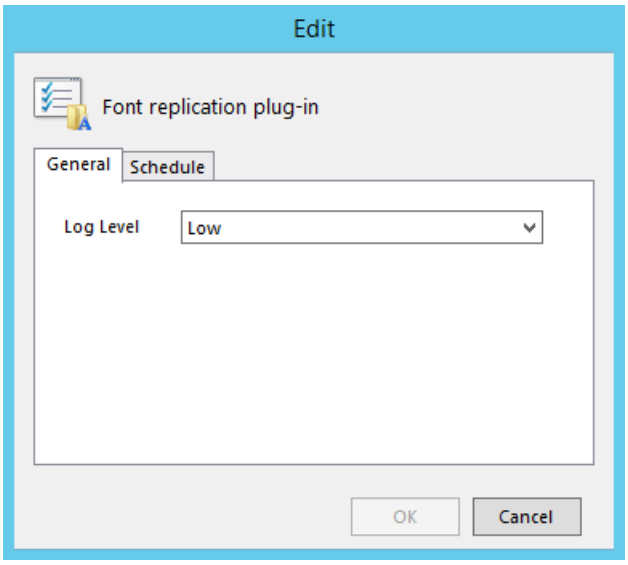
2. Under **Properties & Settings**, click **Components**.



3. Click to select the **Font replication plug-in** and then click **Properties**.

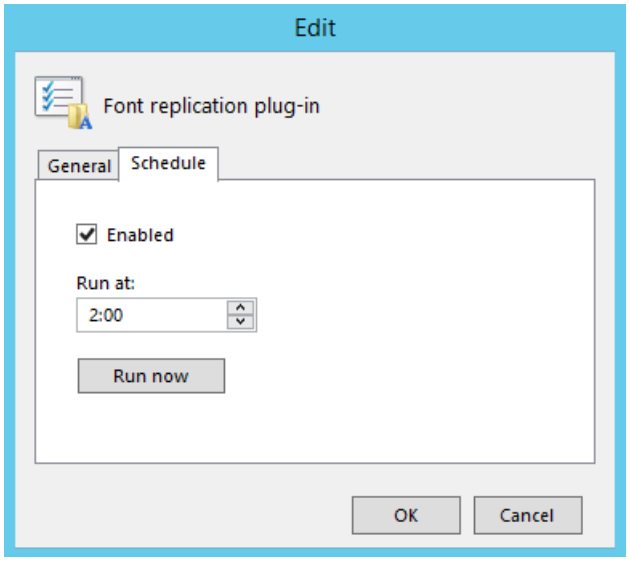


4. Click the **Schedule** tab.



5. Select **Enabled**.

6. Enter a time for the UniPrint Print Server to replicate newly installed fonts from the UniPrint Application Server(s). Default time is set to 02:00 AM.



7. Click **OK** or to replicate fonts on demand, click **Run now**.

Configuring Printer Profiles

Printer profiles are created on the UniPrint Print Server and can be used to enable advanced printer properties such as stapling, hole punching, binding,

etc., that some printers support since it directly accesses the native printer driver.

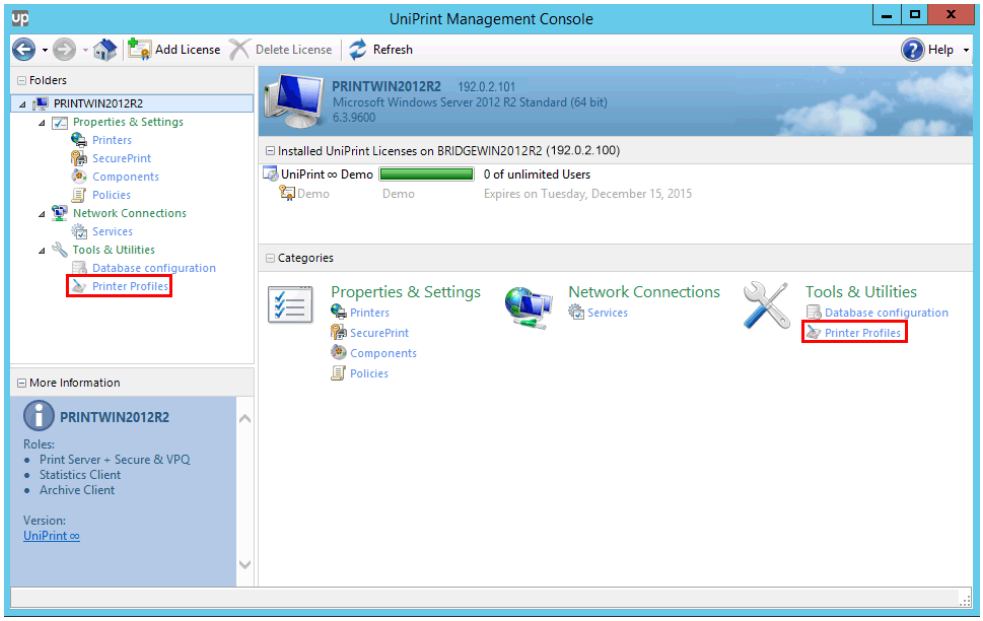
The Printer Profiles can also be selected from the vPad after the user has sent the print job to the UniPrint VPQ. Also the administrator has the ability to create default printer profiles such that if the user does not select an alternate profile, their print job will automatically output using the default printer profile. Default profiles are not user-selectable.

NOTE: If a printer is renamed on the print server, any Printer Level profiles previously created for that printer will no longer be visible. A new printer profile would need to be created for the new printer name.

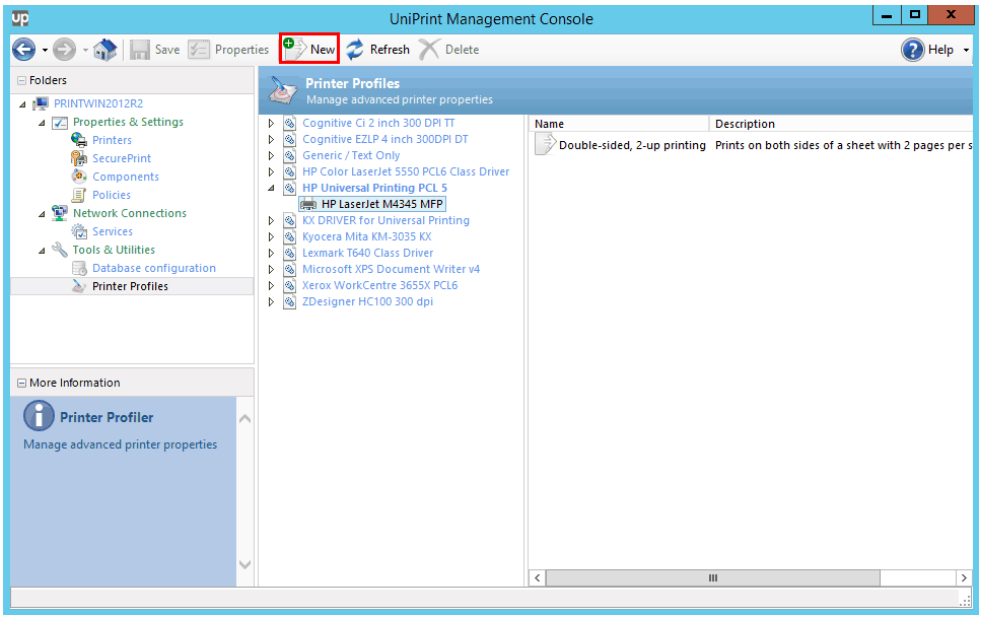
Creating a New Printer Profile

1. On the UniPrint Print Server, open the **UniPrint Management Console**.

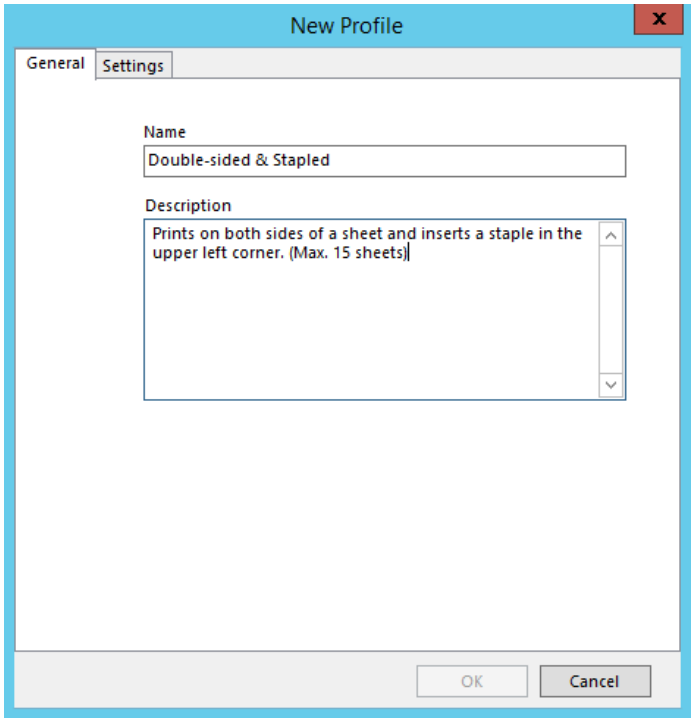
2. Under **Tools & Utilities**, click **Printer Profiles**.



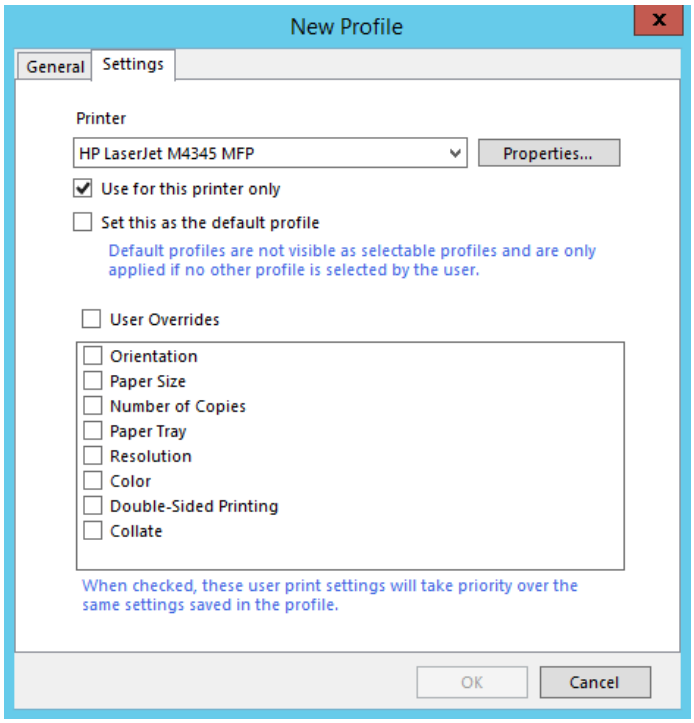
3. Click to select a printer and then click **New**.



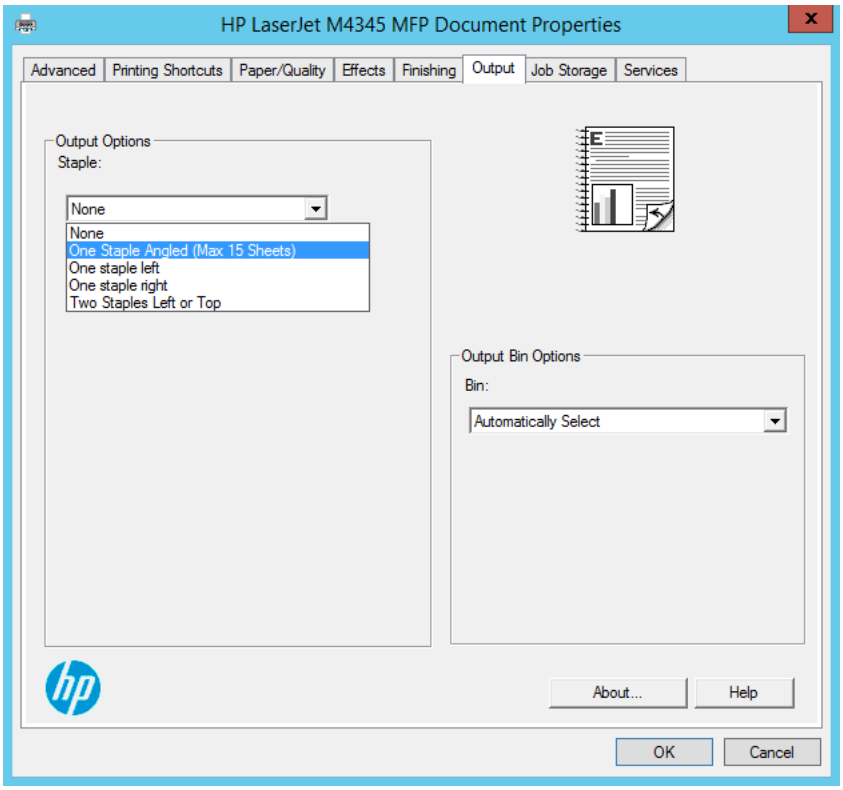
4. Enter a name and description for the new printer profile and then click the **Settings** tab.



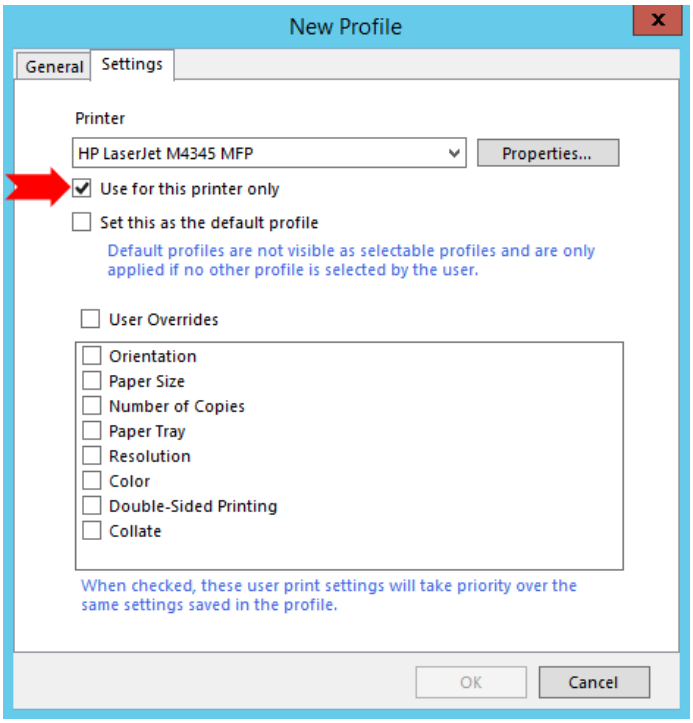
5. Click **Properties**.



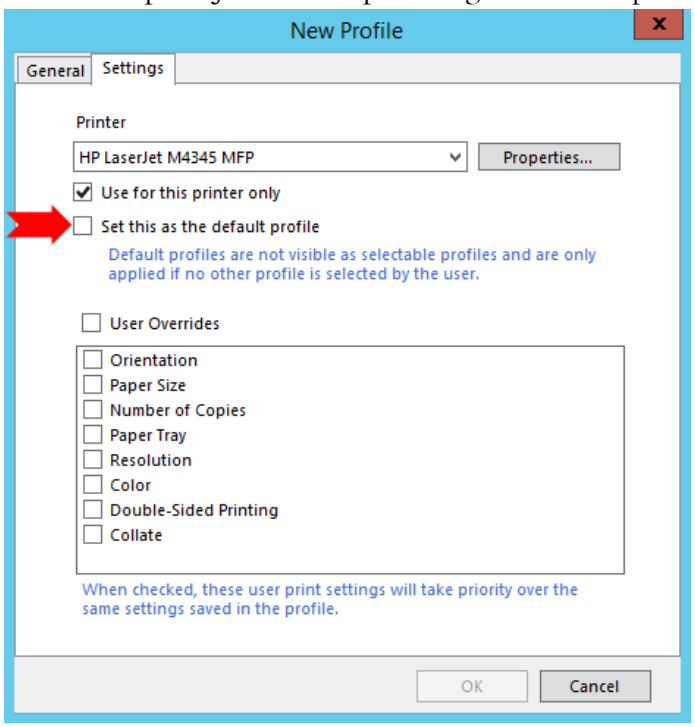
6. The native printer driver will launch. Enable or disable the appropriate properties and then click **OK**.



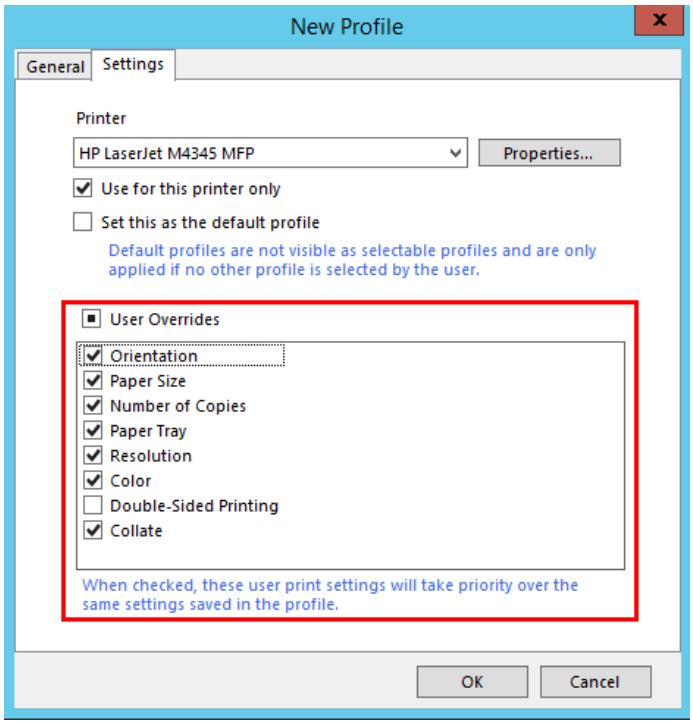
7. If you want this profile to only be applied to the selected printer then select **Use for this printer only**.



8. If you want this to be the default profile, then select **Set this as the default profile**. Default profiles don't appear in the profiles list and users cannot select them. However, if a profile is not selected by the user then their print job will output using the default profile settings.

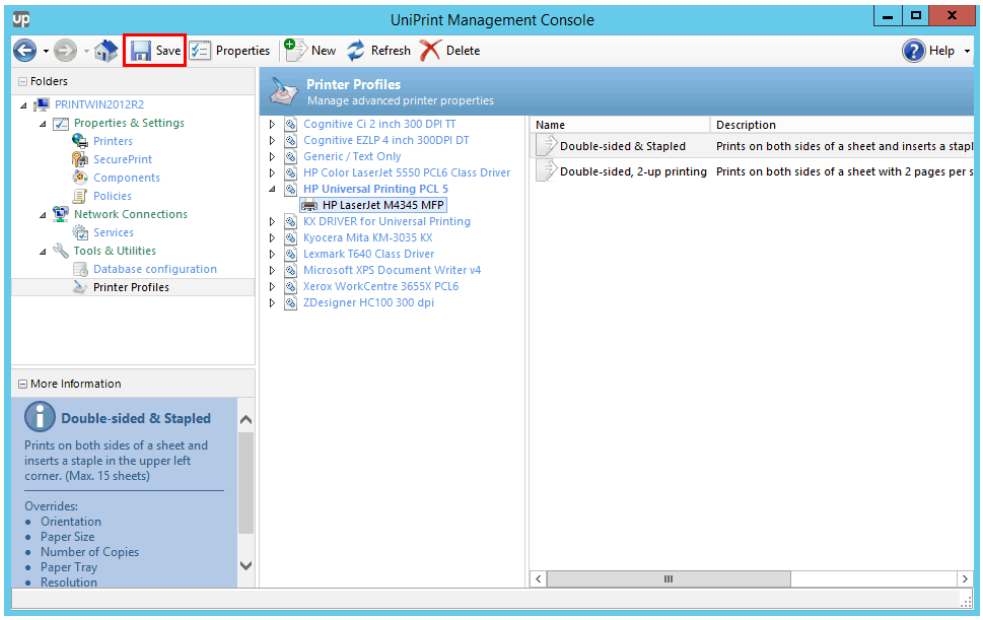


9. Click **User Overrides** and then clear a printer property to prevent the user from overriding it. For example, in this profile we want to enforce double-sided printing, so clear **Double-Sided Printing**. If the user wants the document to be single-sided only, they would have to select a different profile since they cannot override this property.



10. Click **OK**.

11. Click **Save**.



NOTE: Certain printer drivers do not adhere to standard Windows methods of resolving print document properties. In these obscure cases, properties set by the user will be ignored during printing.

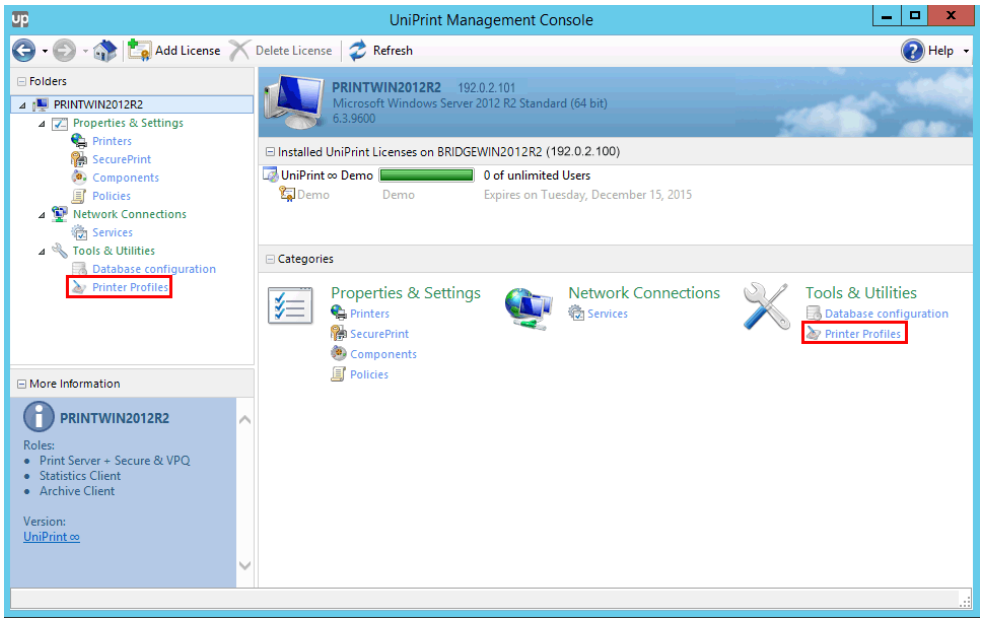
Example: The HP Universal Printing series of drivers ignore the standard Windows "Duplex" (double-sided printing) setting and replace this functionality with HP-specific, non-disclosed settings. Since this setting is "hidden" from Windows applications, the "Duplex" print option set by the user will be ignored and profile settings will be applied.

Recommended Resolution: Create two similar printer profiles. The first profile enables the "Duplex" option and the second profile disables the "Duplex" option.

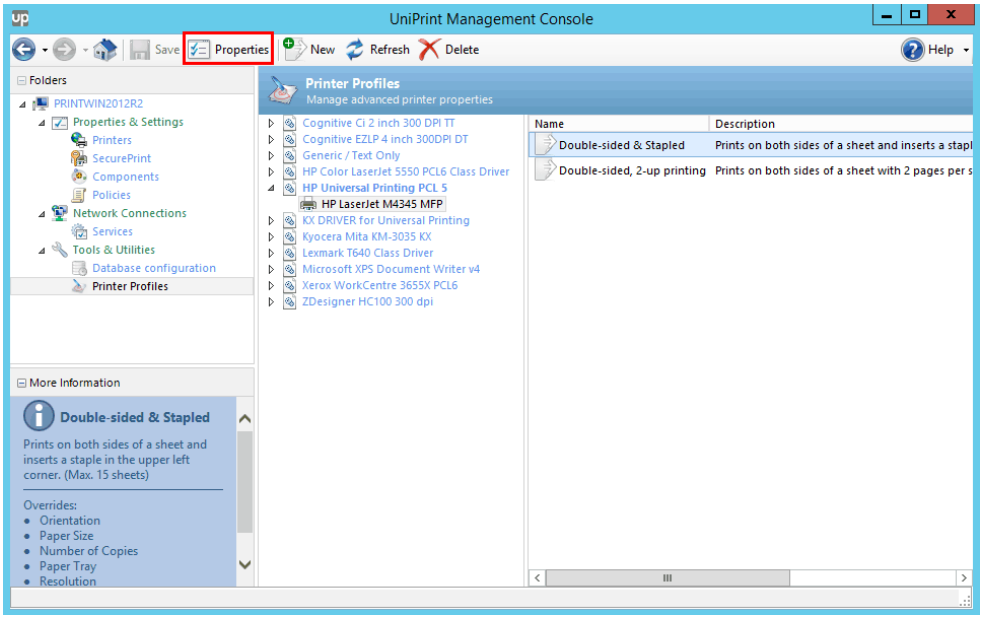
Editing an Existing Printer Profile

1. On the UniPrint Print Server, open the **UniPrint Management Console**.

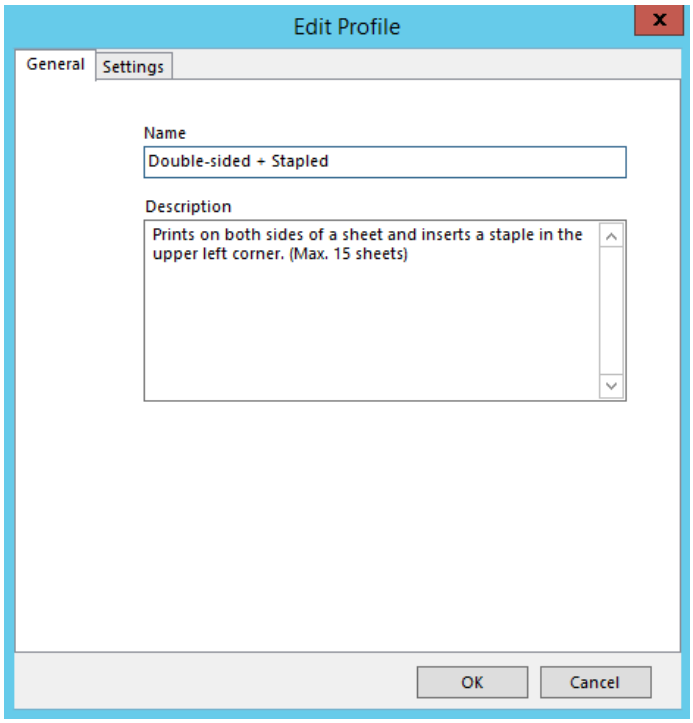
2. Under **Tools & Utilities**, click **Printer Profiles**.



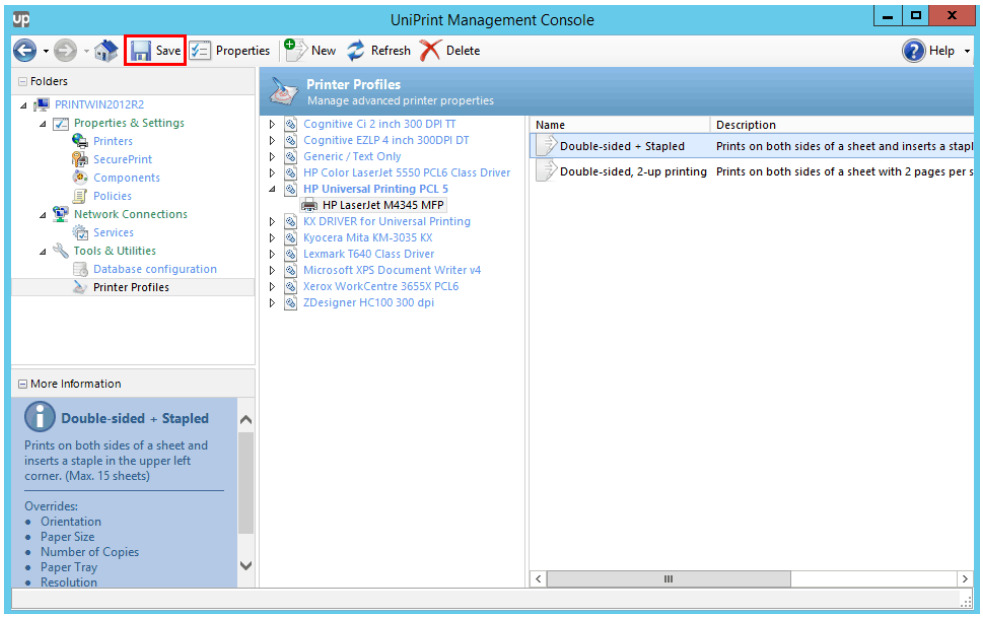
3. Click to select a printer profile and then click **Properties**.



4. Edit the properties, name and/or description and then click **OK**.



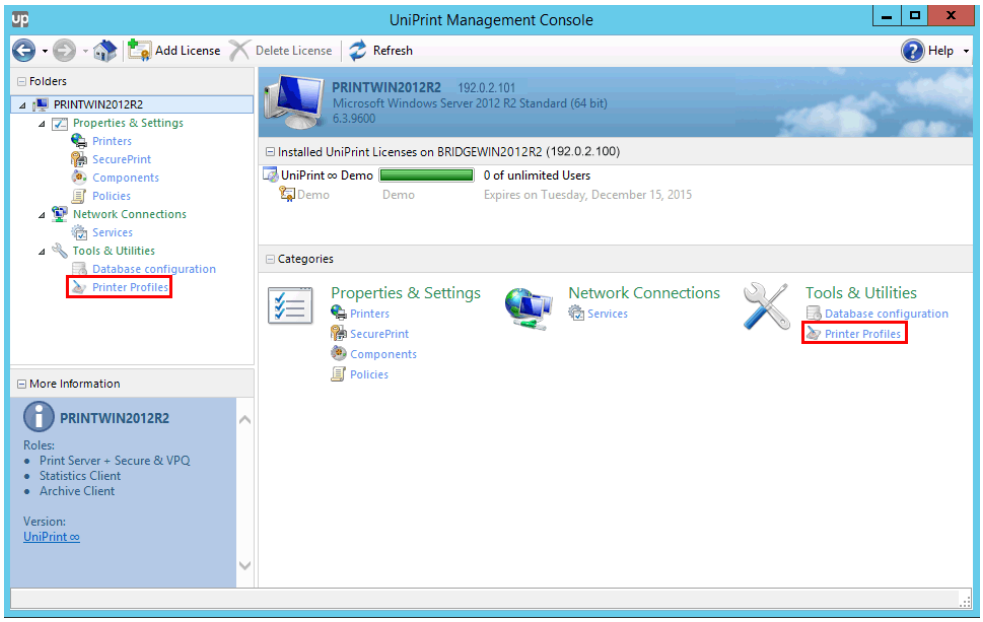
5. Click **Save**.



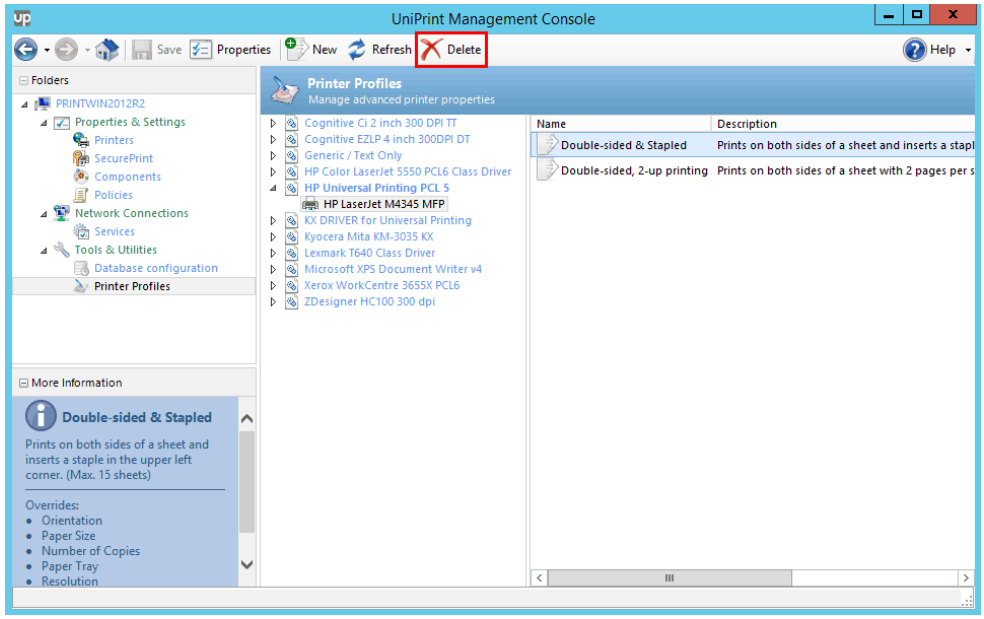
Deleting a Printer Profile

1. On the UniPrint Print Server, open the **UniPrint Management Console**.

2. Under **Tools & Utilities**, click **Printer Profiles**.

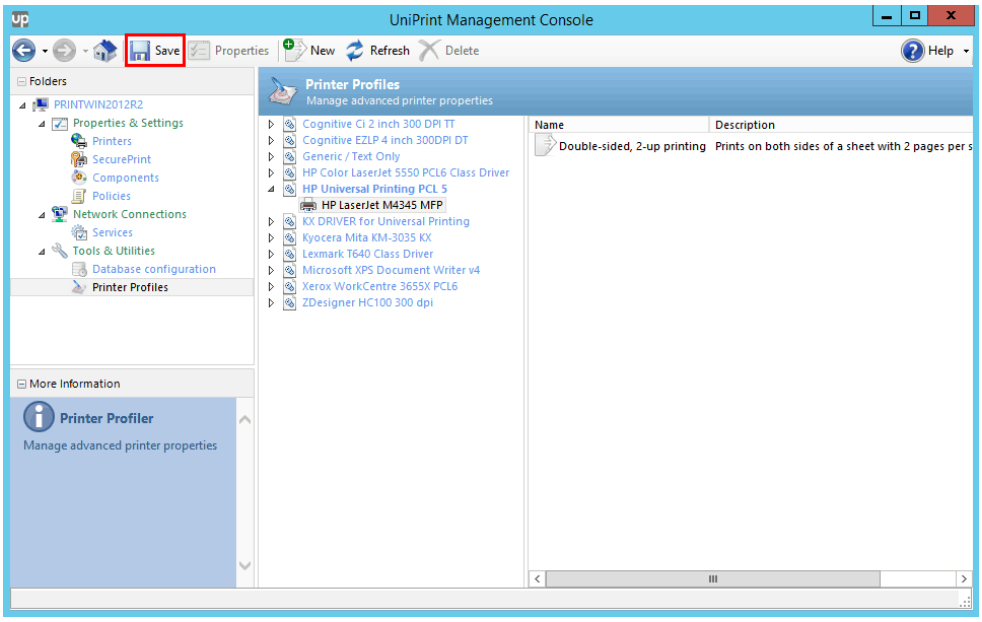


3. Click to select a printer profile to delete and then click **Delete**.



4. Click **Yes** to confirm that you want to delete this profile.

5. Click **Save**.


UniPrint Management Console
Save
Properties
New
Refresh
Delete
Help
Folders
PRINTWIN2012R2
Properties & Settings
Printers
SecurePrint
Components
Policies
Network Connections
Services
Tools & Utilities
Database configuration
Printer Profiles
More Information
Printer Profiler
Manage advanced printer properties
Printer Profiles
Manage advanced printer properties
Cognitive Ci 2 inch 300 DPI TT
Cognitive EZLP 4 inch 300DPI DT
Generic / Text Only
HP Color LaserJet 5550 PCL6 Class Driver
HP Universal Printing PCL 5
HP LaserJet M4345 MFP
KX DRIVER for Universal Printing
Kyocera Mita KM-3035 KX
Lexmark T640 Class Driver
Microsoft XPS Document Writer v4
Xerox WorkCentre 3655X PCL6
ZDesigner HC100 300 dpi
Name
Description
Double-sided, 2-up printing
Prints on both sides of a sheet with 2 pages per s

CHAPTER 5

UniPrint Infinity

Configuring UniPrint Application Server

From the UniPrint Application Server, UniPrint printer properties can be configured globally for all users, the usage of group policies can be prioritized and which UniPrint features your users will have access to in their sessions can be set. The Adobe Plug-in can also be configured to replace the Print function in Adobe Reader/Acrobat to Print to UniPrint.

NOTE: Some antivirus programs may block some UniPrint Infinity files. It is recommended that the folder that contains the UniPrint Infinity files, for example, **C:\Program Files\UniPrint Suite,** be added to the exclusion list in the antivirus program.

BEST PRACTICE: For client devices connecting to the Application Server, it is recommended that IPv6 be disabled on all client devices.

Preparing UniPrint for Custom Forms

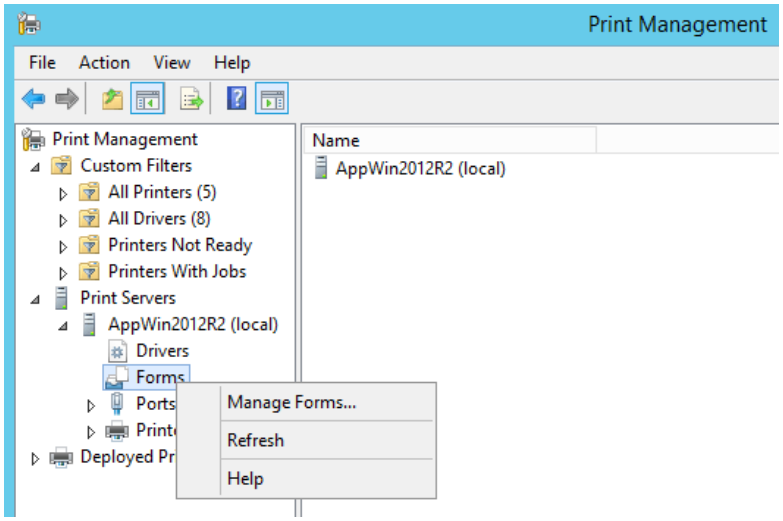
Custom forms, for example labels and invitation cards, are not available in standard paper sizes. These non-standard paper sizes need to be defined on the Application Server prior to printing to them.

Defining a custom Form on the Application (Citrix/RDS) Server

Before you can use custom forms, they first need to be defined on the Application Server.

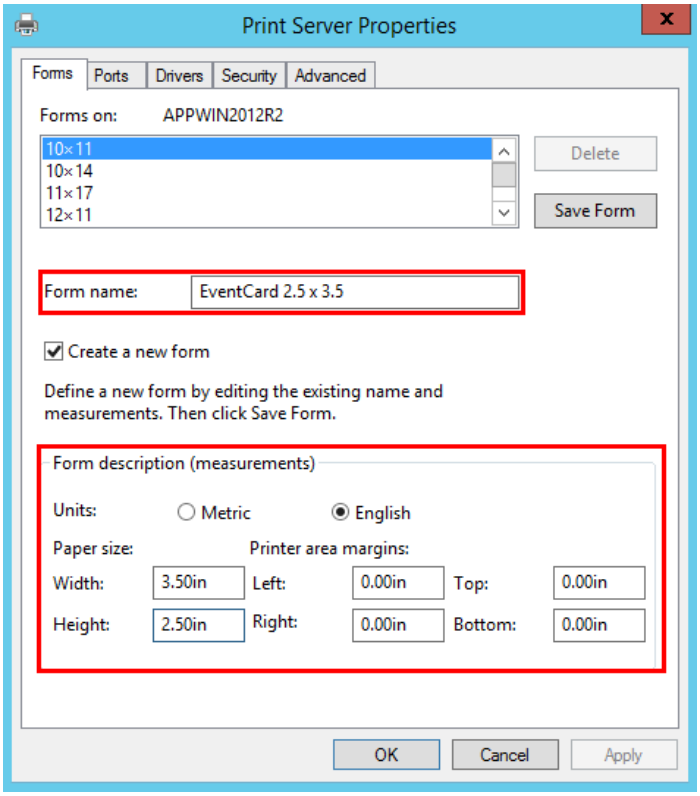
1. Click **Start**, click the **Control Panel** tile and then double-click **Print Management**.

2. In the console tree, expand **Print Servers**, click the applicable Application Server, right-click **Forms** and then select **Manage Forms**.



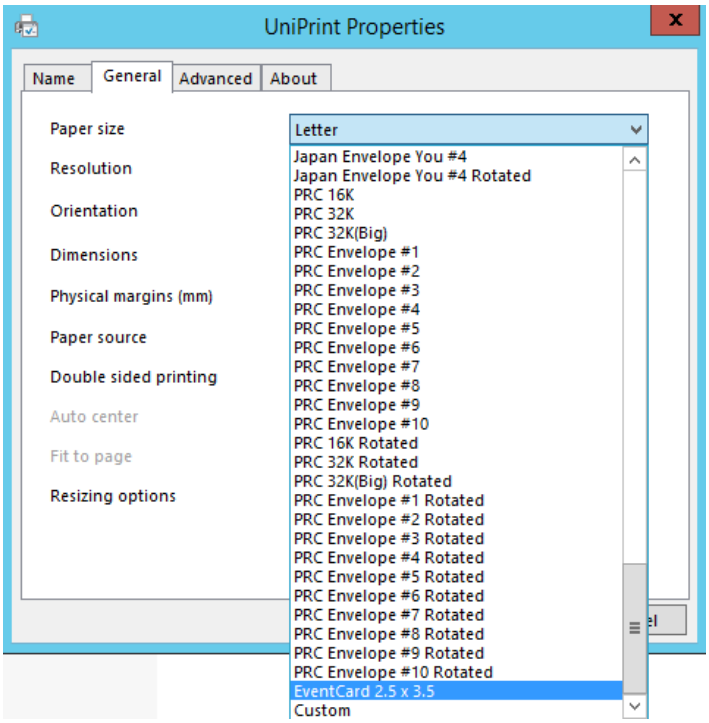
3. Select **Create a new form.**

4. Enter a **Form name** and the appropriate measurements.



5. Click **Save Form** to create the custom form.

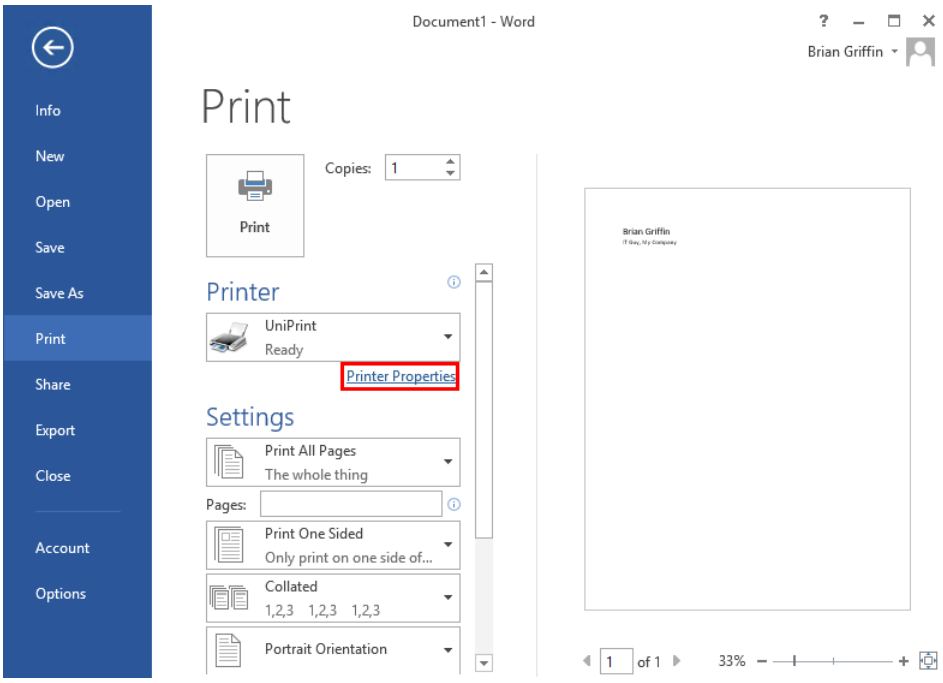
Once the custom form is defined on the Application Server, it will be available in UniPrint printer **Paper Size** list.



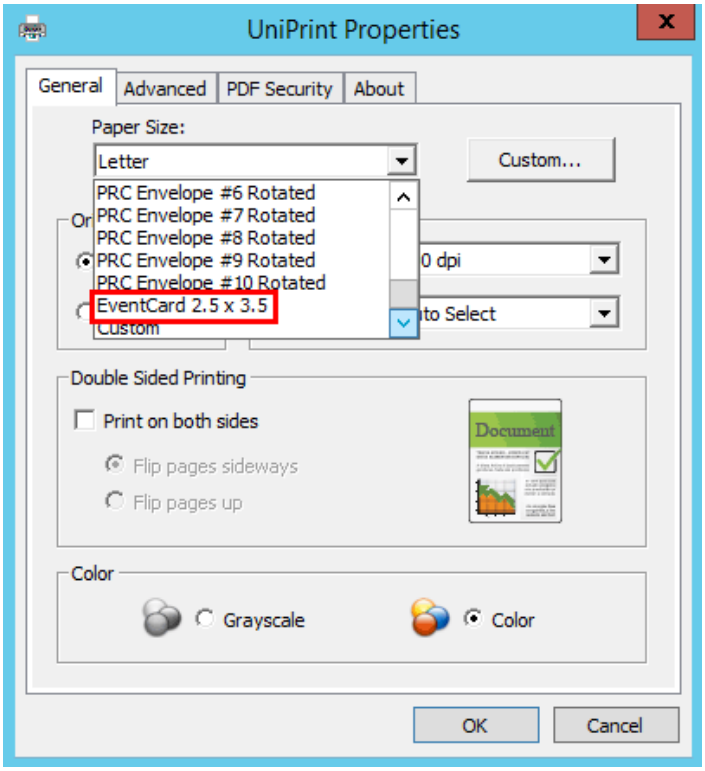
Using a Custom Form in a User Session

1. Log on to your Application Server and open an application, for example Microsoft Word.

2. Ensure that **UniPrint** is selected from the printer list and then click **Printer Properties**.



3. From the **Paper Size** list, select the custom form that was defined on the Application Server.

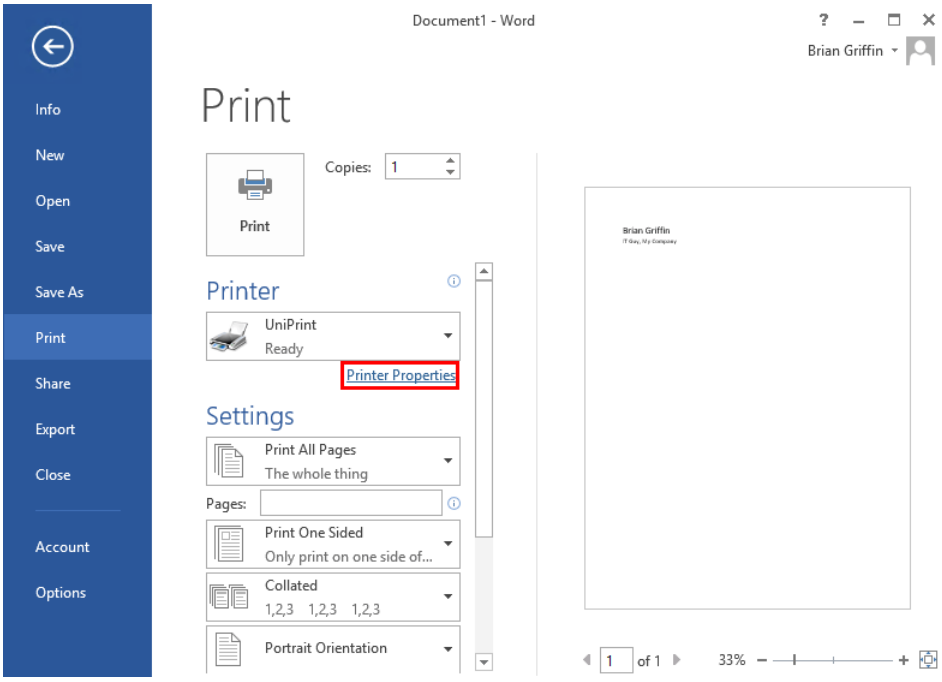


4. Click **OK**.

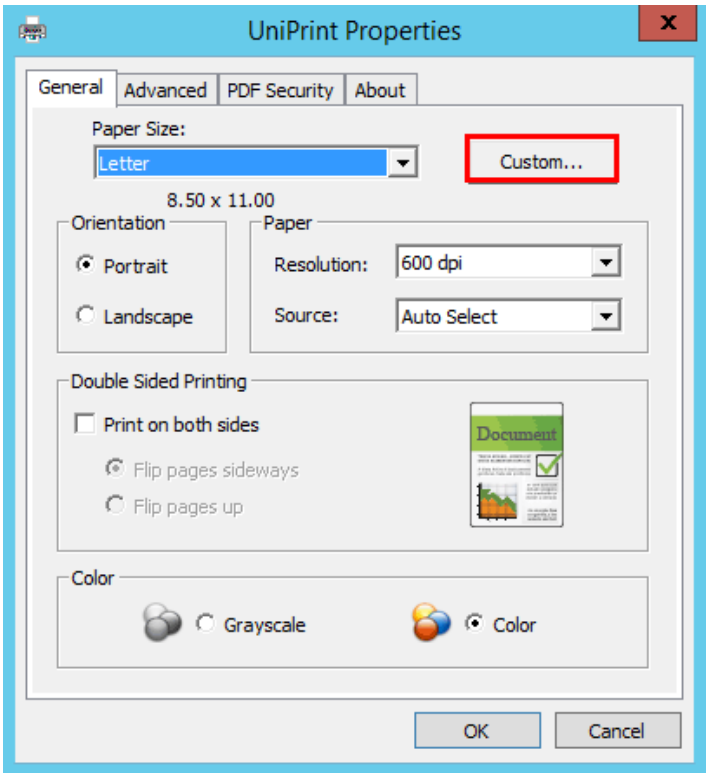
Defining a Custom Form in a User Session

1. Log on to your Application Server and open an application, for example Microsoft Word.

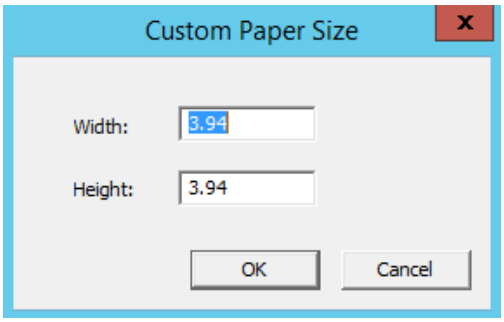
2. Ensure that **UniPrint** is selected from the printer list and then click **Printer Properties**.



3. Click **Custom**.



4. Specify the **Width** and **Length** and then click **OK**.



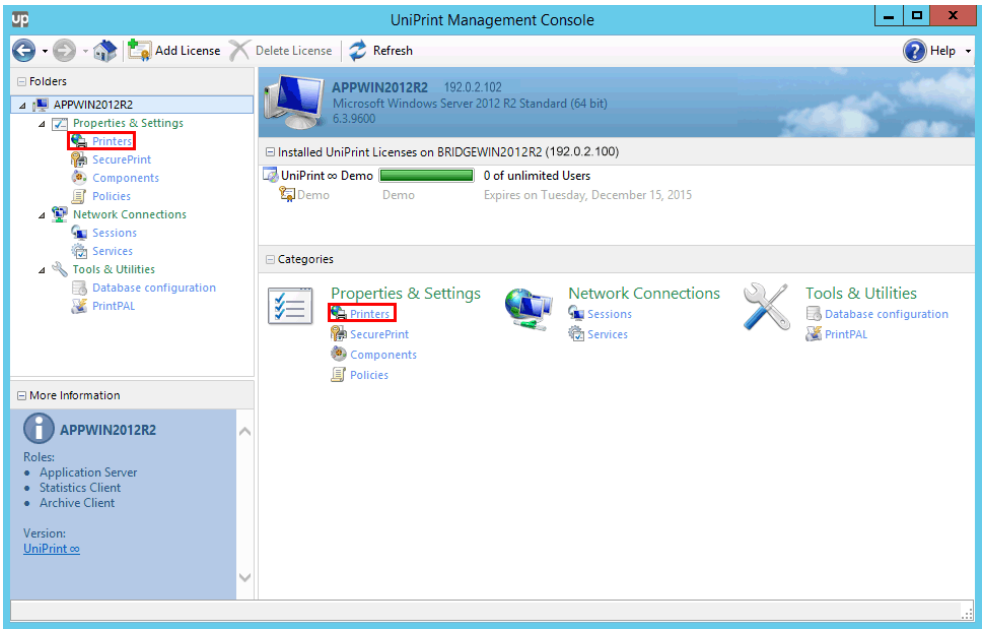
5. Click **OK** again.

Changing UniPrint Printer Properties Globally For All Users

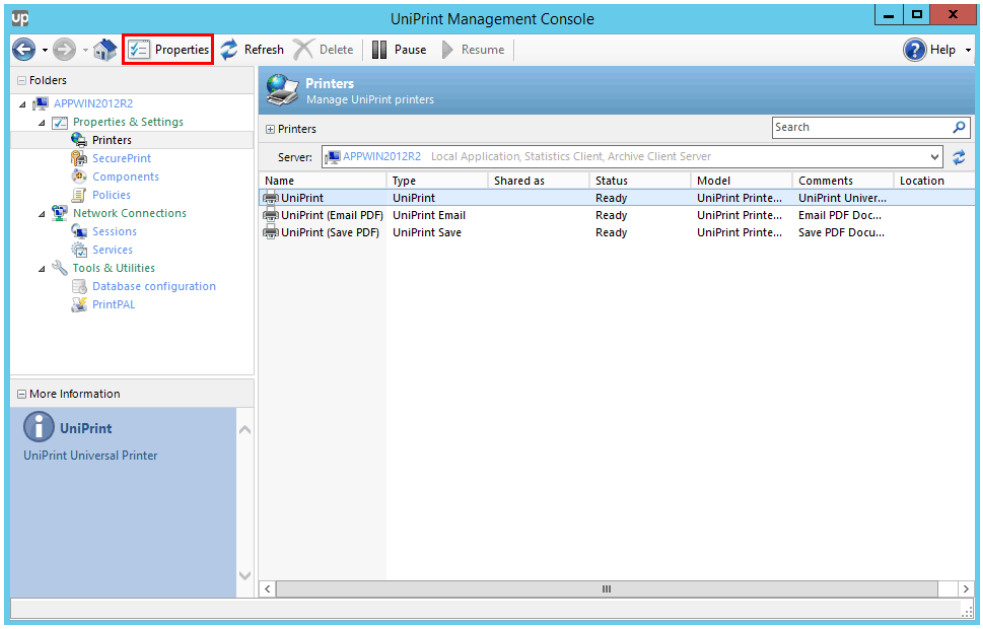
To set UniPrint printer properties globally for all users who logon to this server, do the following:

1. On the Application Server, open the **UniPrint Management Console**.

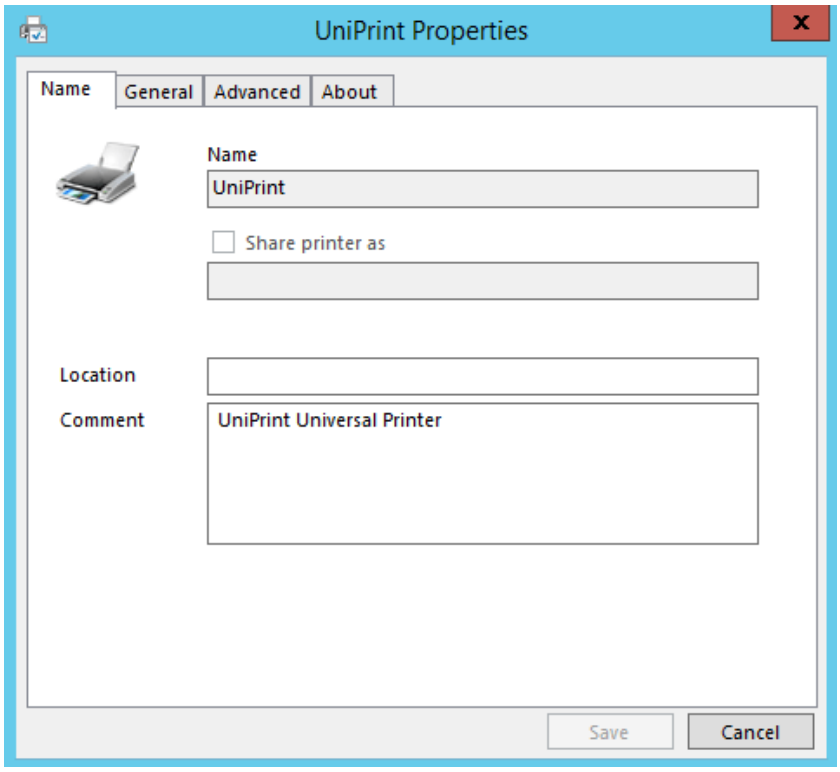
2. Under **Properties & Settings**, click **Printers**.



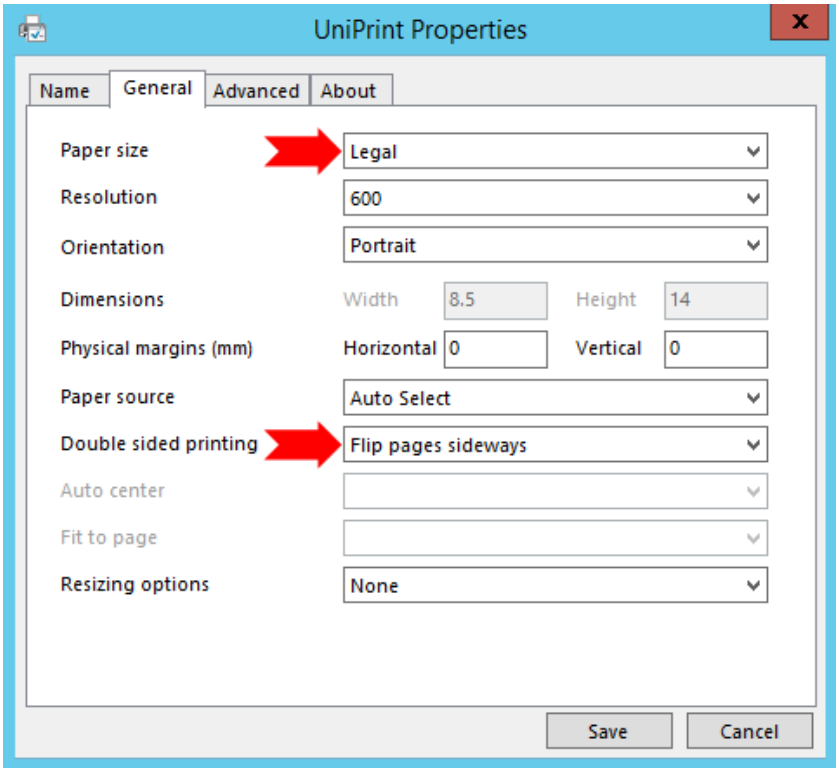
3. Click to select **UniPrint** and then click **Properties**.



4. Click either the **General** or **Advanced** tab.



5. Change the desired properties, for example **Paper size** and **Double-sided printing**, and then click **Save**.



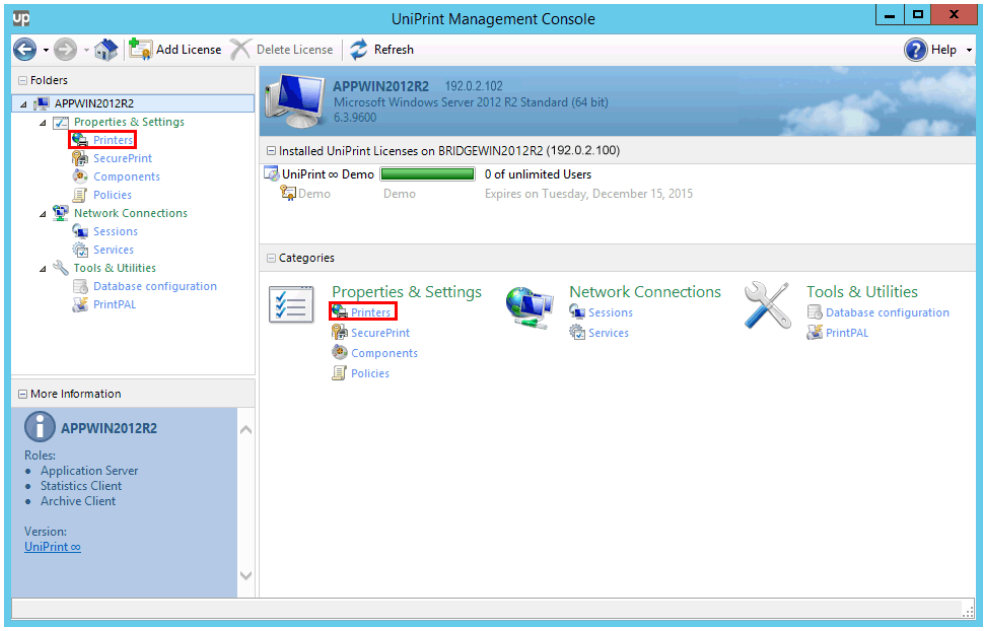
Copying UniPrint Printer Properties to Another Application Server

After configuring the UniPrint printer properties on one Application Server, those properties can then be copied to other Application Servers.

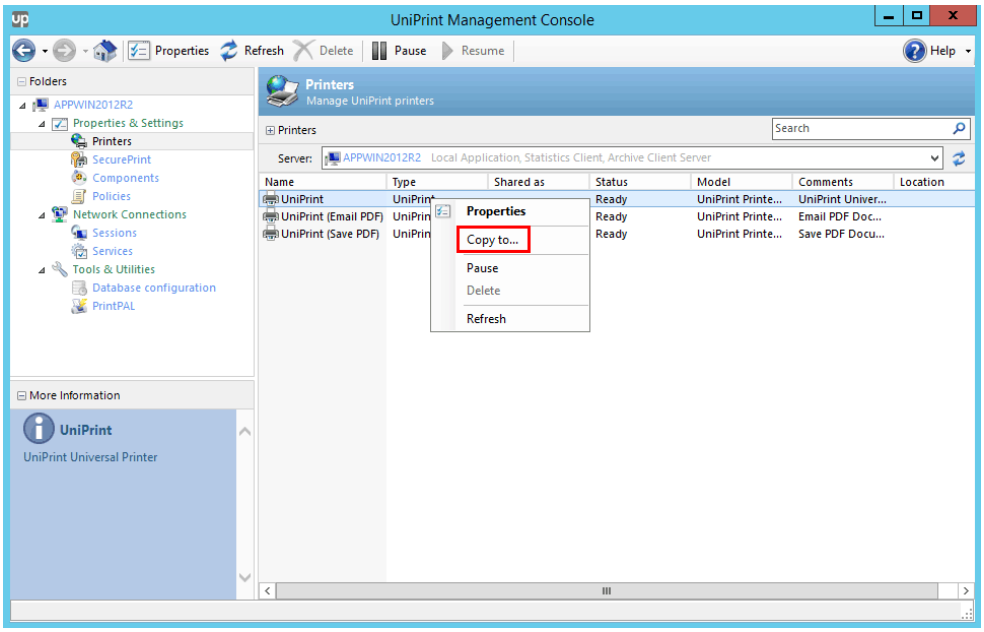
To copy UniPrint printer properties to other Application Servers, do the following:

1. On the UniPrint Application Server, open the **UniPrint Management Console**.

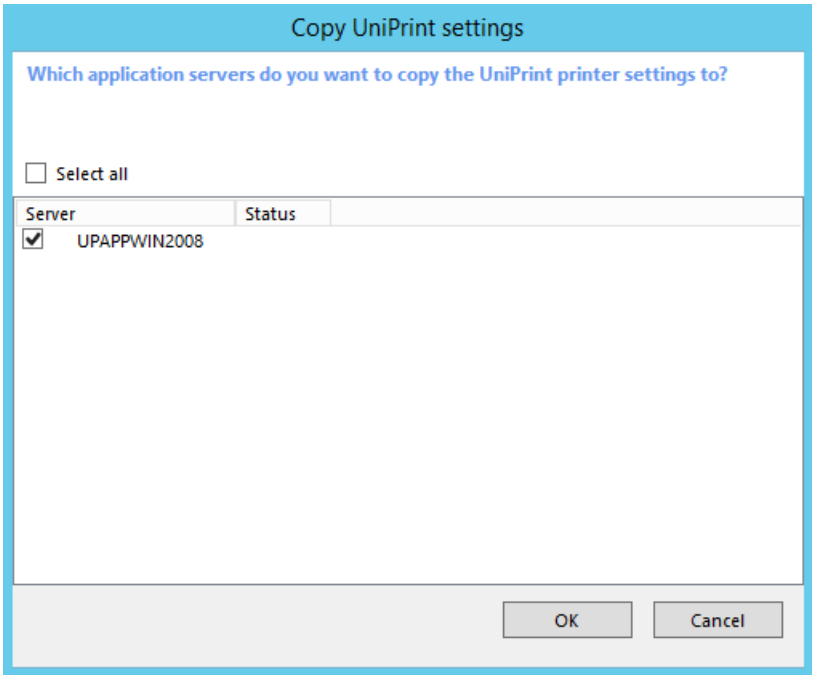
2. Under **Properties & Settings**, click **Printers**.



3. Right-click the **UniPrint** printer and then select **Copy to**.

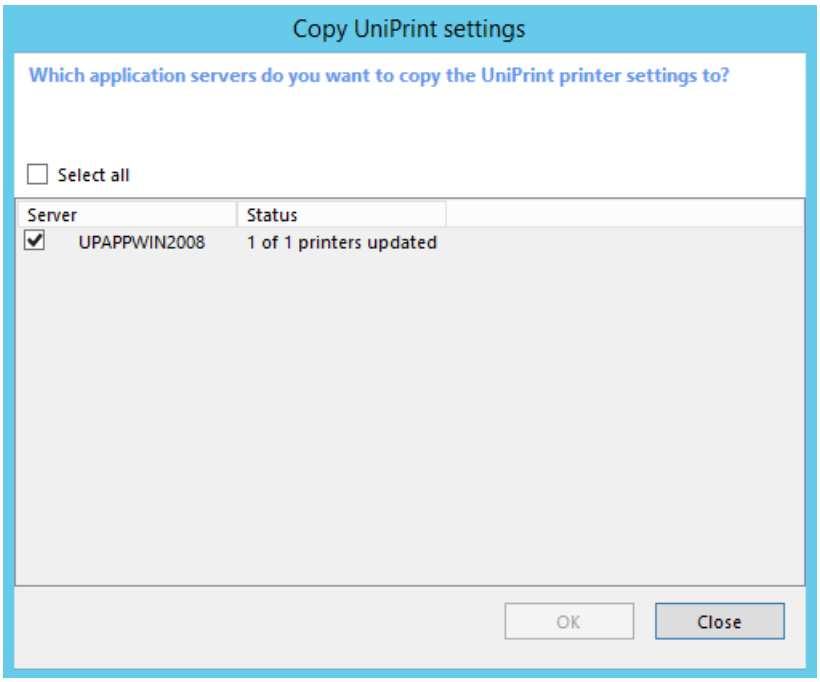


4. Select the Application Server(s) to which you want to copy UniPrint printer properties and then click **OK**.



5. Enter administrative credentials and then click **OK**.

6. UniPrint printer properties will be copied to the selected application server(s). Click **Close**.

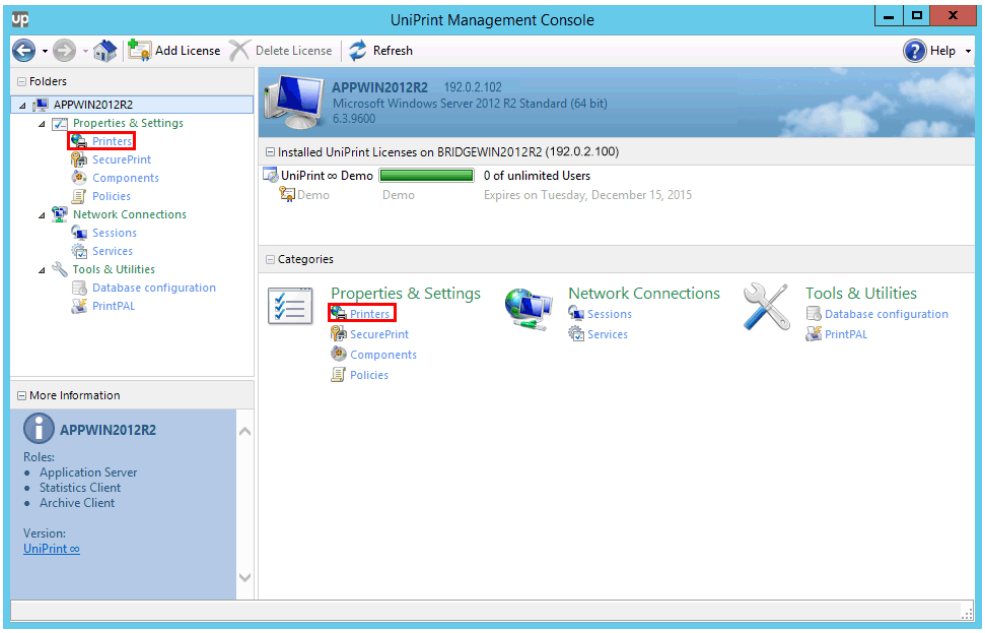


Enabling & Configuring UniPrint To E-mail Print Jobs as PDF Attachments

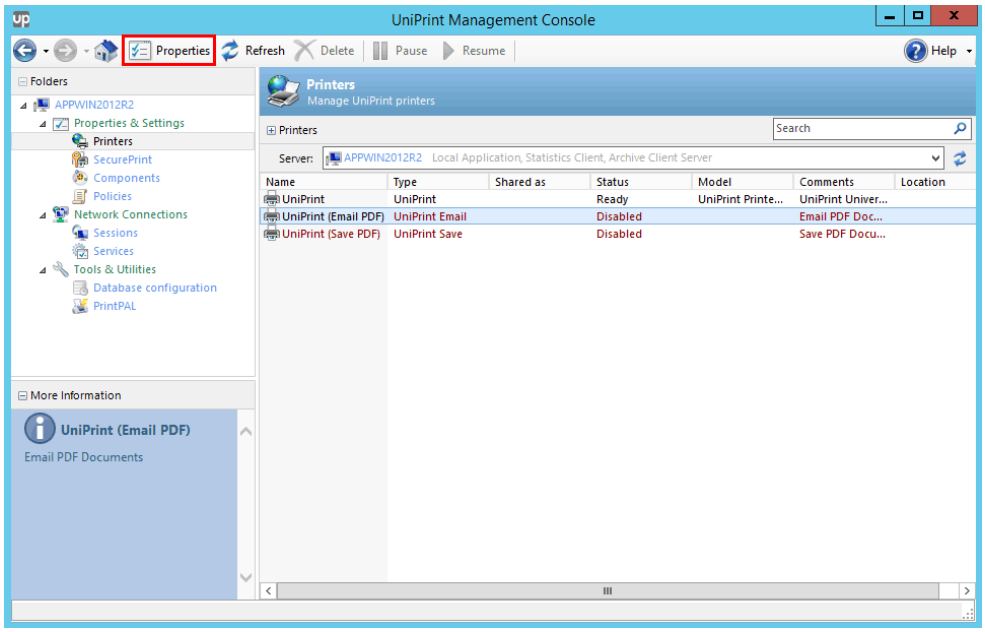
To enable UniPrint to e-mail a print job as a PDF attachment from the UniPrint Application Server, do the following:

1. On the UniPrint Application Server, open the **UniPrint Management Console**.

2. Under **Properties & Settings**, click **Printers**.

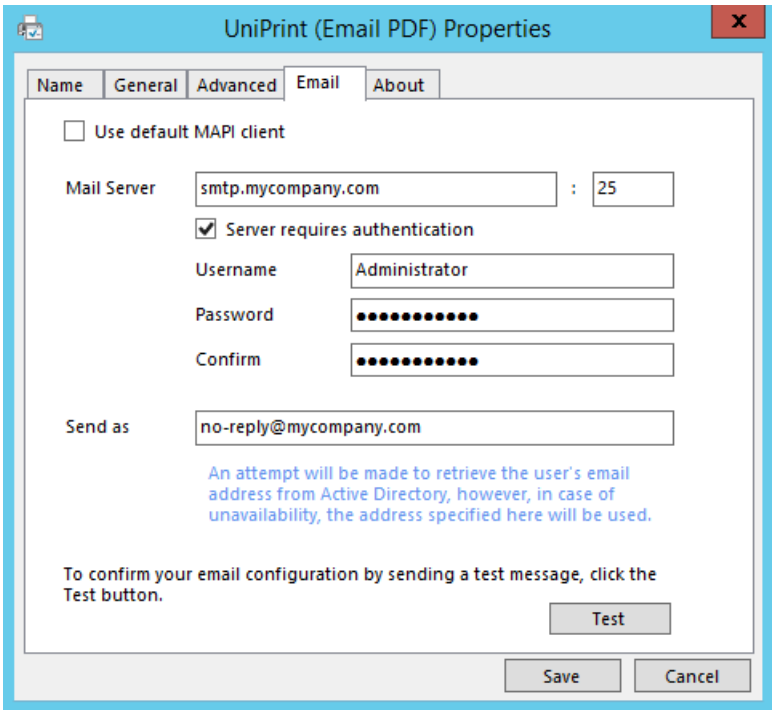


3. Click to select the **UniPrint (Email PDF)** queue and then click **Properties**.



4. To use the default Messaging API client, select **Use default MAPI client** or enter the **Mail Server** address and port number that will be

used to send out e-mail. If the mail server requires authentication, select **Server requires authentication**.



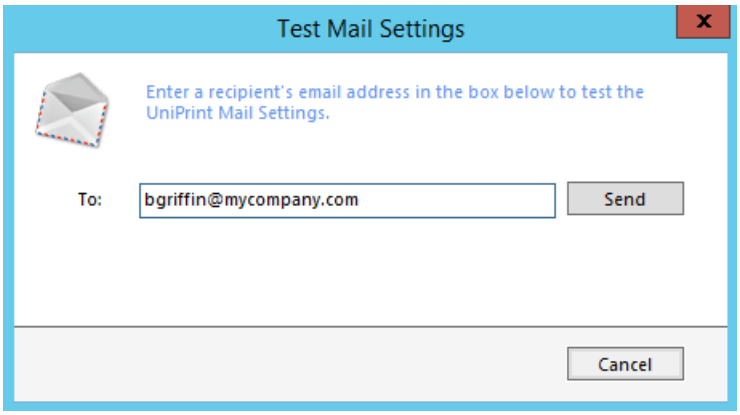
NOTE: As of this release, there is no fix from Microsoft to create a MAPI association with Windows Mail Metro application in Windows 8.1, that allows users to send e-mail attachments in this manner. For more information see http://social.technet.microsoft.com/Forums/en-US/W8ITProPreRel/thread/0ddc6e71-af56-4f98-a186-4b23f9071154.

5. Enter the **Username** and the **Password** twice.

6. Beside **Send As**, enter the e-mail address that will appear in the **From** field and then click **Test** to test these settings.

NOTE: If the user is a domain user and the **Display name** and **E-mail** fields have been populated in Active Directory, then UniPrint will display the address from Active Directory User properties instead of the default address set in **Send as**.

7. Enter an e-mail address and then click **Send**.



8. Click **OK** to clear the message box and then click **Save**.

9. Click **Yes** to enable this queue.

10. Click **Yes** to restart the UniPrint Control Service.

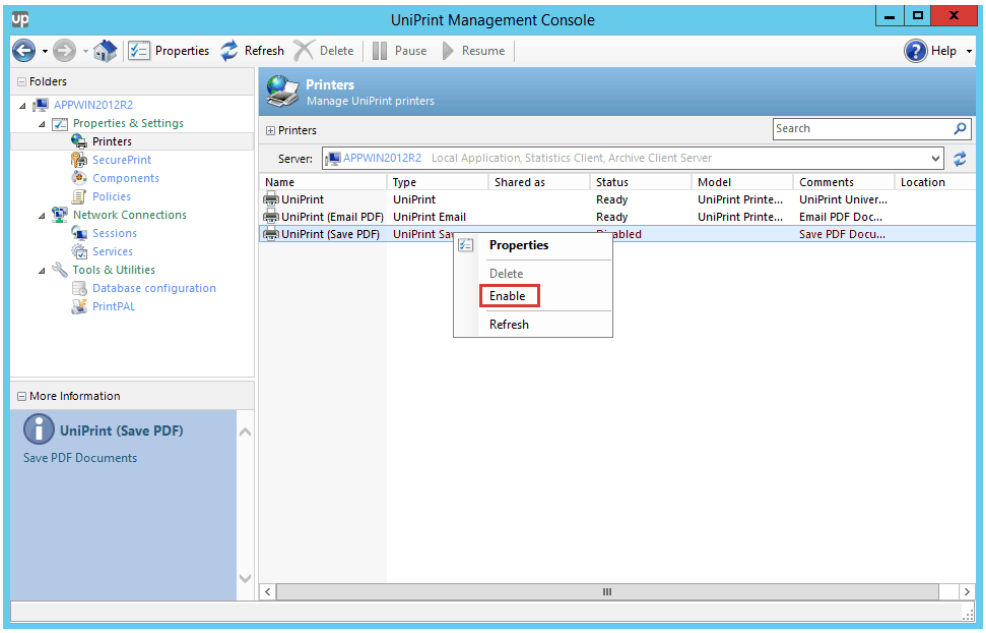
Enabling UniPrint To Save Print Jobs As PDF Files

To allow users to save their print jobs as PDF files to any network accessible location, do the following:

1. On the UniPrint Application Server, open the **UniPrint Management Console**.

2. Under **Properties & Settings**, click **Printers**.

3. Right-click **UniPrint (Save PDF)** and then select **Enable**.



4. Click **Yes** to restart the UniPrint Control Service.

Enabling & Setting Order of Precedence of Group Policy Objects

Administrators can configure how UniPrint applies configuration settings from alternate sources on all UniPrint component servers. Alternate sources include Active Directory group policy and saved user preferences.

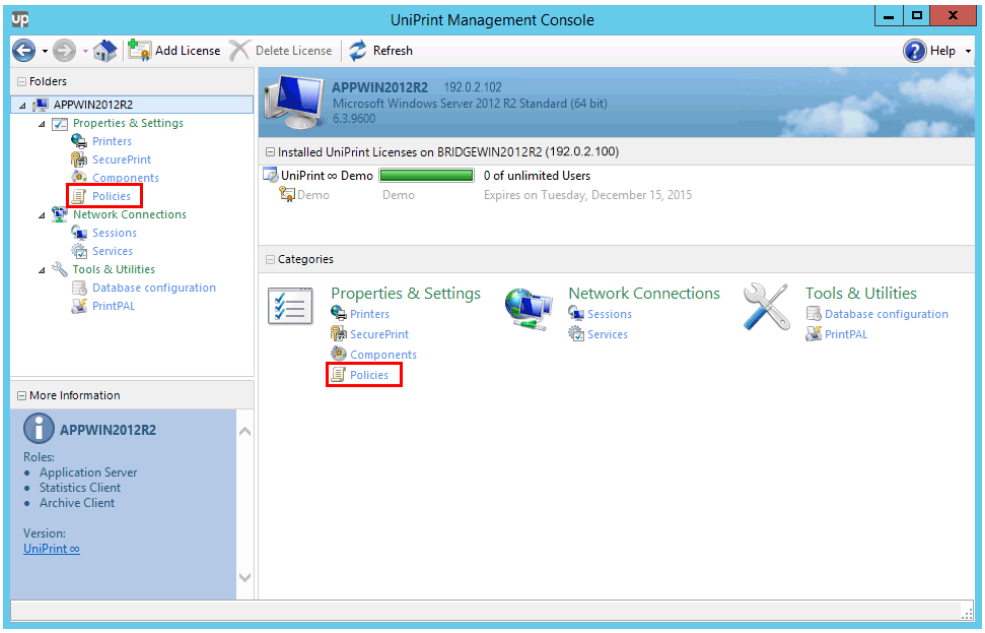
The following figures shown are taken from the UniPrint Application Server, however the instructions can also be applied to the UniPrint Bridge and the UniPrint Print Server.

Enabling Policies

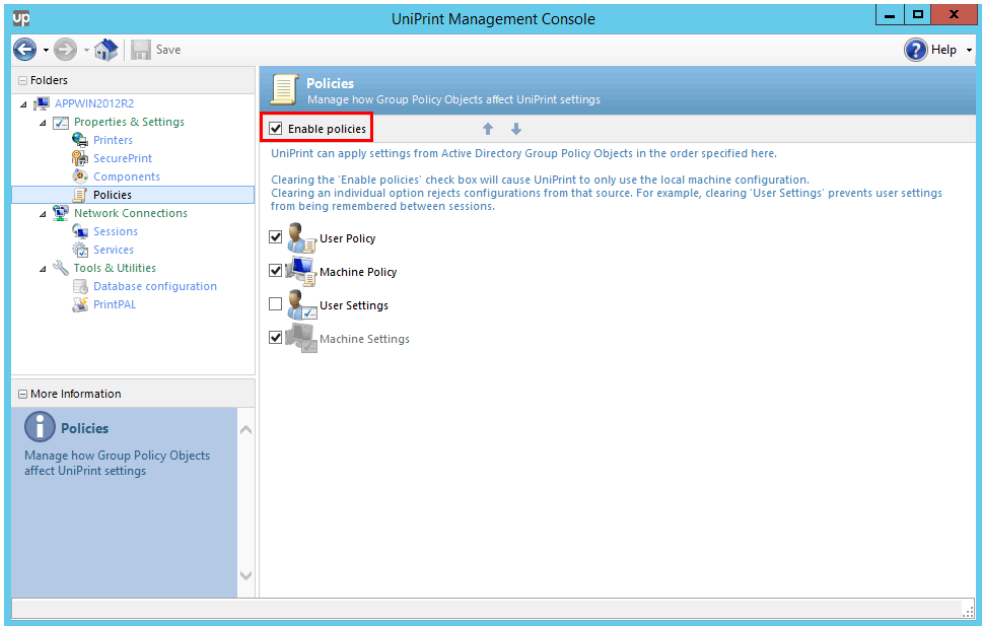
To enable different policy sources, do the following:

1. On a UniPrint component server, open the **UniPrint Management Console**.

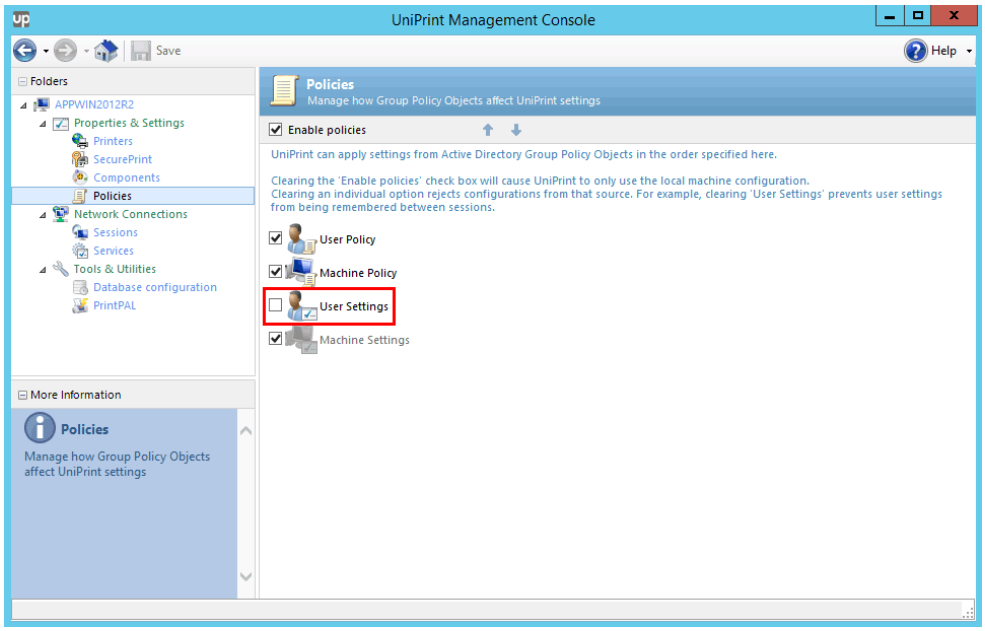
2. Under **Properties & Settings**, click **Policies**.



3. Ensure that **Enable policies** is selected.



4. Click to select a policy to enable, or clear a check box to disable a policy



Configuration Source	Description
User Policy	Configuration settings for specific users or user groups through Active Directory group policy. This policy is only applicable to the UniPrint Application Server.
Machine Policy	Configuration settings for specific UniPrint components through Active Directory group policy.
User Settings	Settings configured by users will be persistent across multiple ICA/RDP sessions. These settings include: Orientation, Page Size, Resolution, Paper Source and Double sided printing. They may, however, be overridden by a group policy listed higher in the processing order. This policy is only applicable to the UniPrint Application Server.
Machine Settings	Default settings configured from the UniPrint Management Console. These settings cannot be disabled and always have the lowest priority. To enforce machine settings, clear all other alternate source check boxes.

5. Click **Save**.

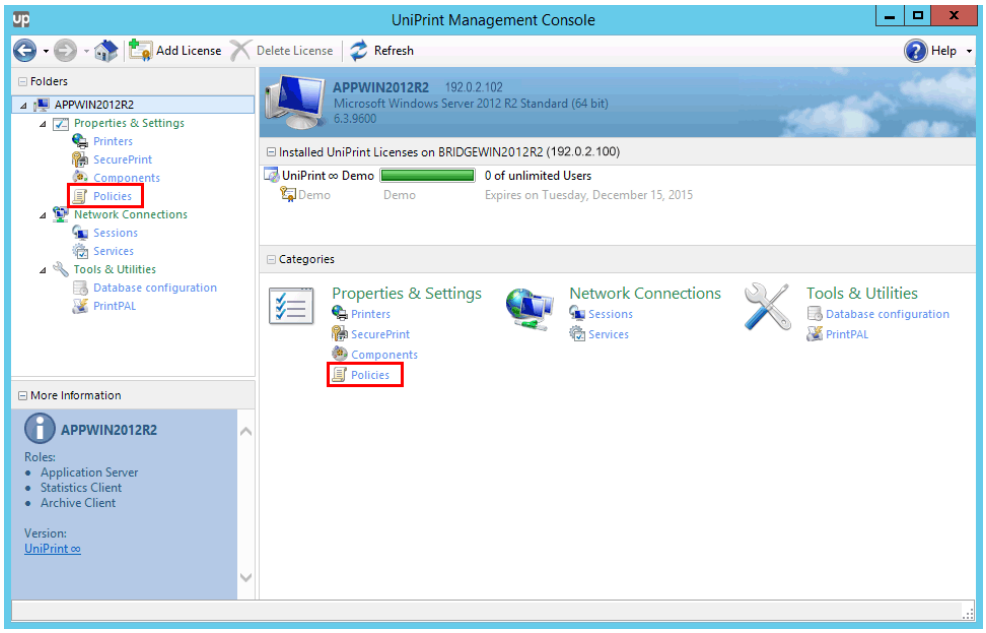
Forcing UniPrint Infinity to Apply Settings Only From The Management Console

For debugging purposes, you may want to prevent UniPrint Infinity from applying configuration settings from alternate sources such as Active Directory and force it to use only the settings set in the Management Console.

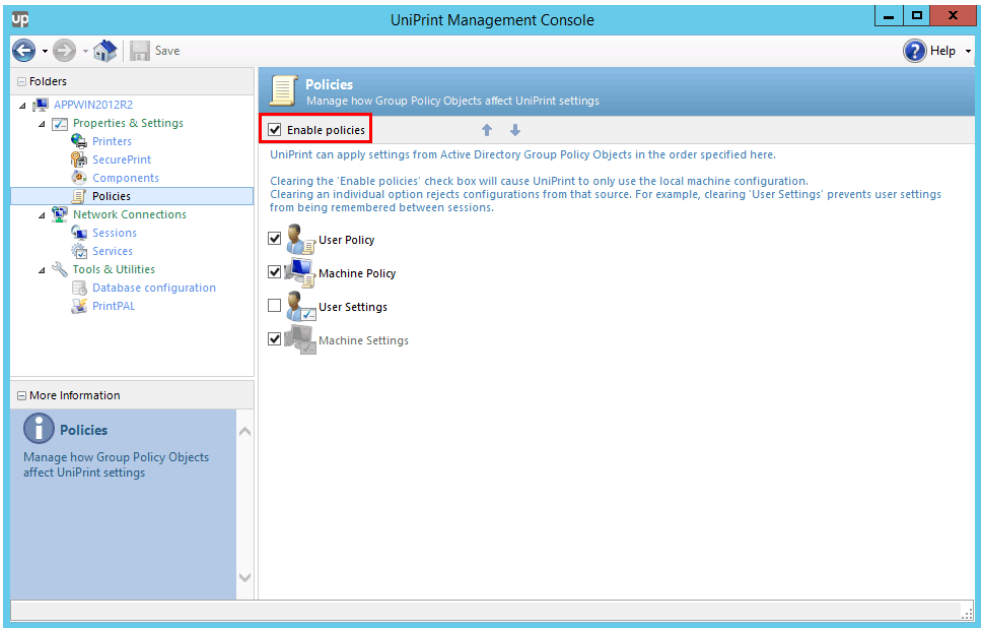
To force UniPrint Infinity to use settings from the UniPrint Management Console, do the following:

1. On a UniPrint component server, open the **UniPrint Management Console**.

2. Under **Properties & Settings**, click **Policies**.



3. Clear **Enable policies**.



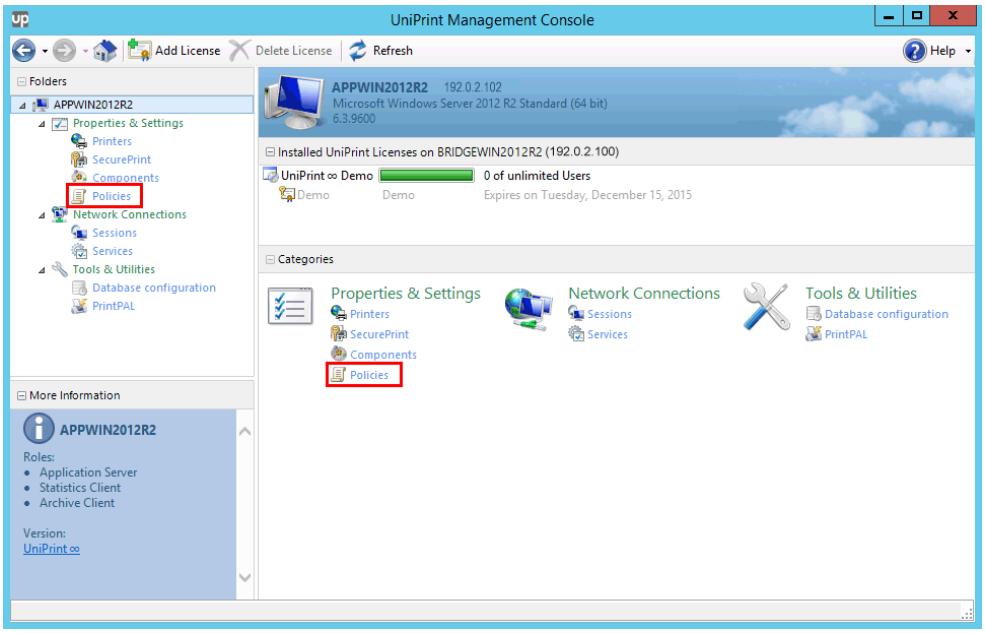
4. Click **Save**.

Changing the Order of Precedence

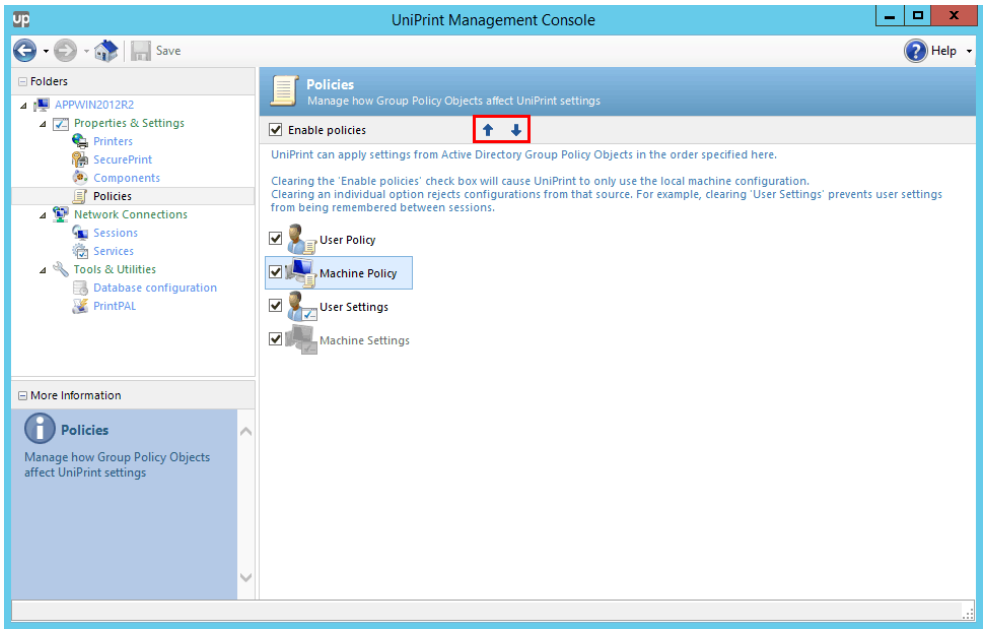
You can change the order in which configuration settings are applied. The settings at the top of the list will always override the ones set below them. To change order of precedence, do the following:

1. On a UniPrint component server, open the **UniPrint Management Console**.

2. Under **Properties & Settings**, click **Policies**.



3. Click to select a policy and then click either the **UP** or **DOWN** arrow.



4. Click **Save**.

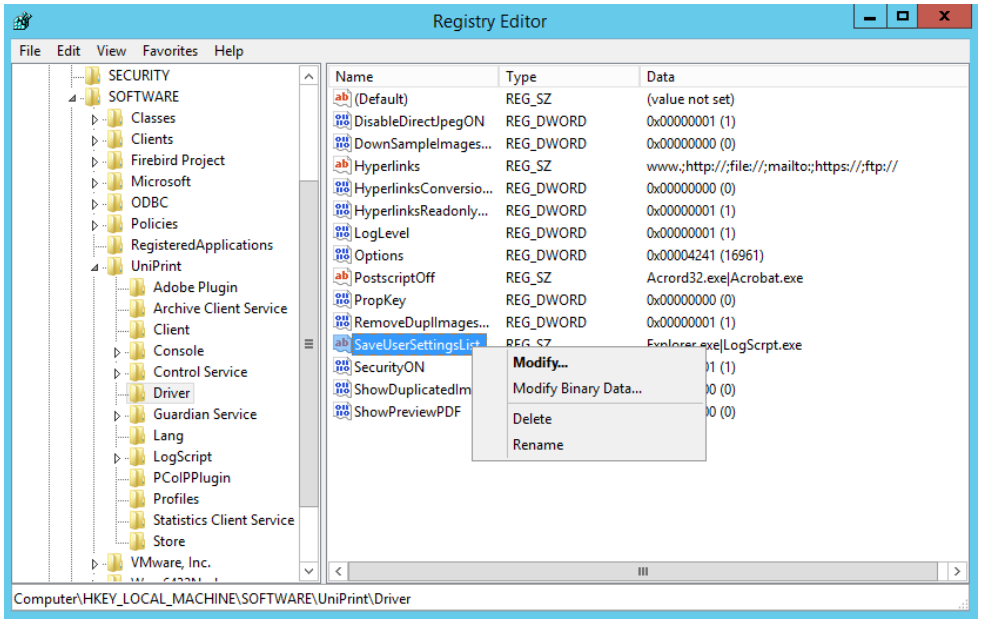
Enabling Applications to Save User Settings With UPSession

In environments where users are not allowed to access Printers and Faxes through the Control Panel, user settings can still be saved through UPSession for individual applications.

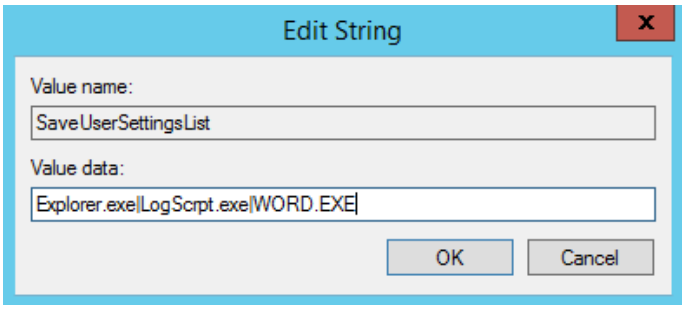
To enable applications to save current user settings to the registry, do the following:

1. On the Application Server, open the registry editor.

2. Under the key, **HKEY_LOCAL_MACHINE\SOFTWARE\UniPrint\Driver**, right-click the registry value, **SaveUserSettingsList** and then click **Modify**.



3. Enter a list of application executable files, separated by | (pipe) and then click **OK**.



Enabling UniPrint Session Features

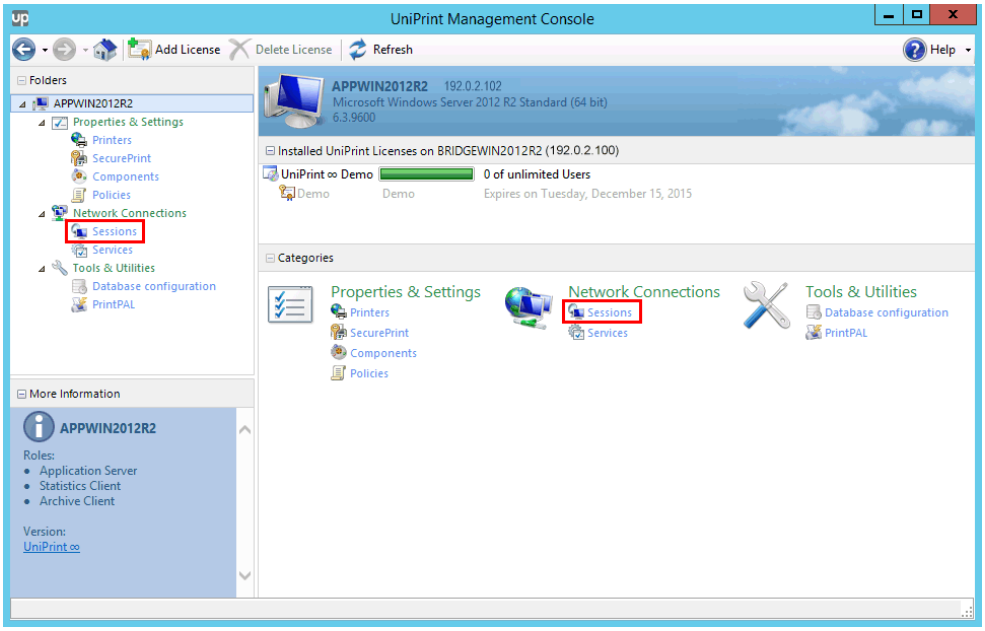
Setting Which Protocols Are Used To Transfer Print Jobs To The UniPrint Client

Based on the connecting client's protocol, UniPrint creates a private, protocol-specific virtual channel between the Application Server and the endpoint device for transferring rendered print jobs.

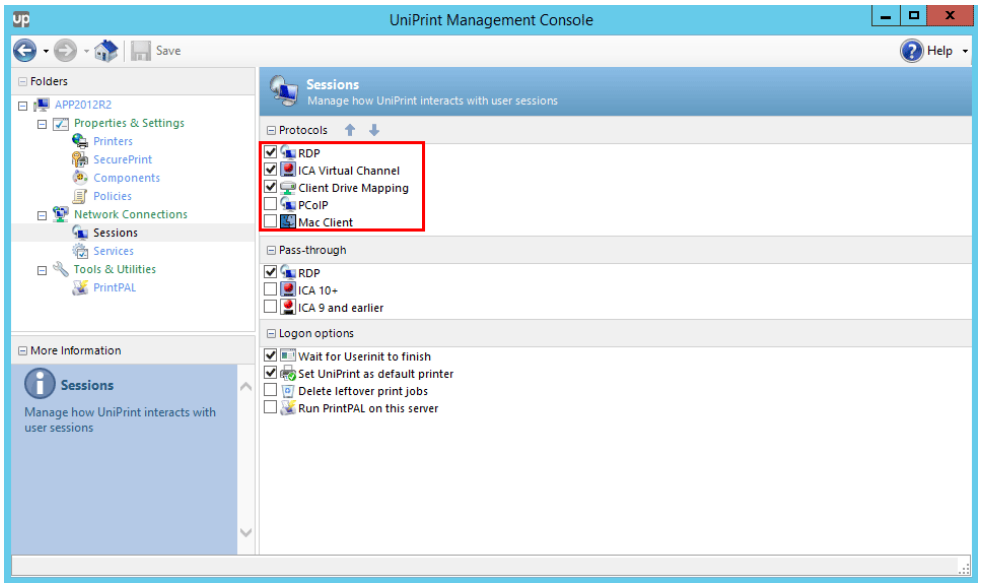
To enable the creation of a specific virtual channel, do the following:

1. On the UniPrint Application Server, open the **UniPrint Management Console**.

2. Under **Network Connections**, click **Sessions**.



3. Click to select a protocol or transfer method.



Protocol	Description/Notes
RDP	Remote Desktop Protocol. RDP does not require Citrix to be installed on the Application Server.
ICA Virtual Channel	Citrix Independent Computing Architecture. ICA does not require client drive mapping to be enabled on the Citrix server.
Client Drive Mapping	Requires client drive mapping to be enabled on the Citrix server and is compatible with both Windows and non-Windows clients.
PCoIP	PC Over IP. Supports PCoIP for Teradici and VMware Horizon View in VDI deployments. UniPrint Client 5.3 or later must be installed on the endpoint device for PCoIP to work.
Mac Client	Allows a Macintosh computer to access an Application Server.

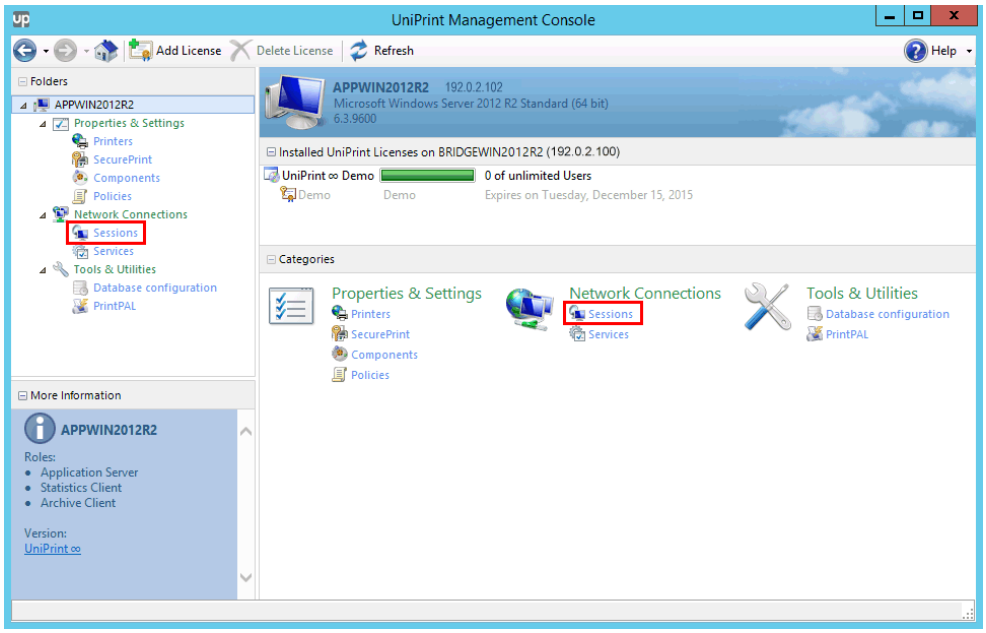
4. Click **Save**.

Changing the Order That UniPrint Infinity Uses For Auto-detecting Transfer Protocols

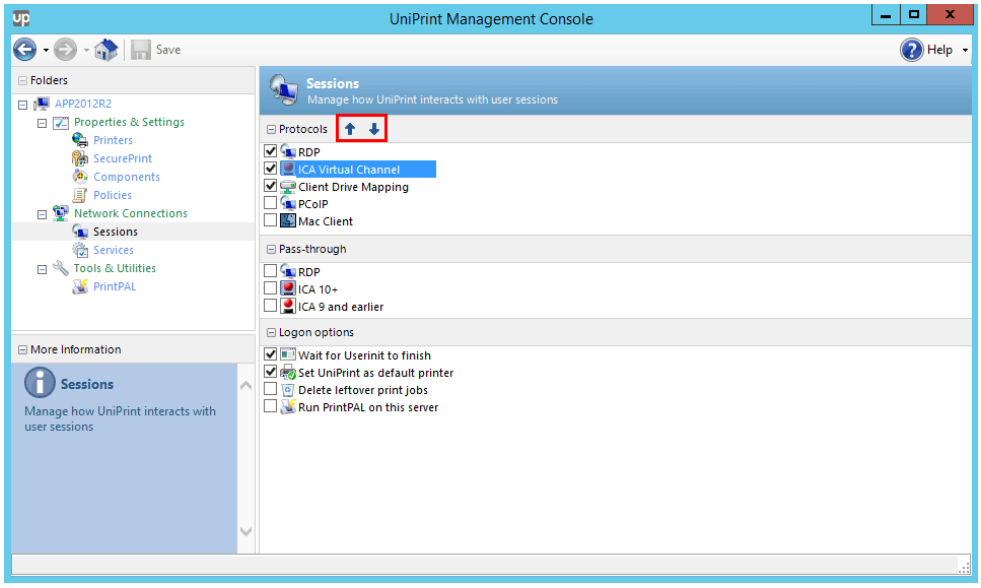
To change the order UniPrint Infinity uses when auto-detecting the transfer protocol, do the following:

1. On the UniPrint Application Server, open the **UniPrint Management Console**.

2. Under **Network Connections**, click **Sessions**.



3. Click to select a protocol to promote or demote and then click the **UP** or **DOWN** arrows.



4. Click **Save**. Only the first detected transfer protocol is used.

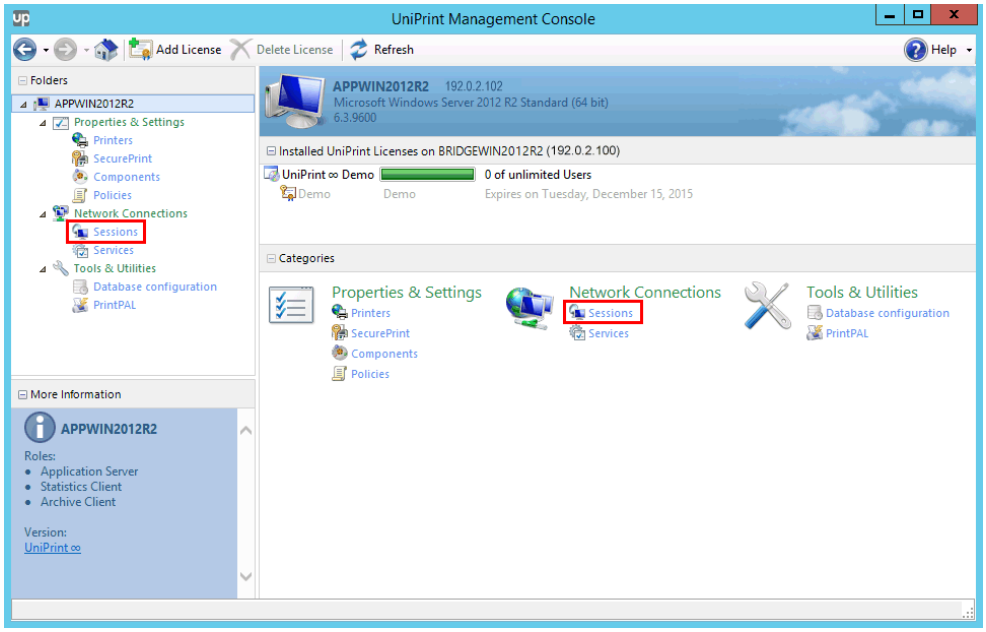
Setting This Application Server As A Pass-through Client

UniPrint Infinity can be configured such that this Application Server will act as a pass-through client, routing print jobs printed from another Application Server that has UniPrint Application Server installed. As a pass-through client, UniPrint spools print jobs through nested ICA/RDP sessions where users connect from one ICA/RDP session to another by launching a second ICA/RDP session within their original session. Pass-through printing allows UniPrint to send print jobs seamlessly through multiple ICA/RDP sessions back to the first client workstation in the chain. Only the originating client device host name and IP address are passed on to the other nested sessions.

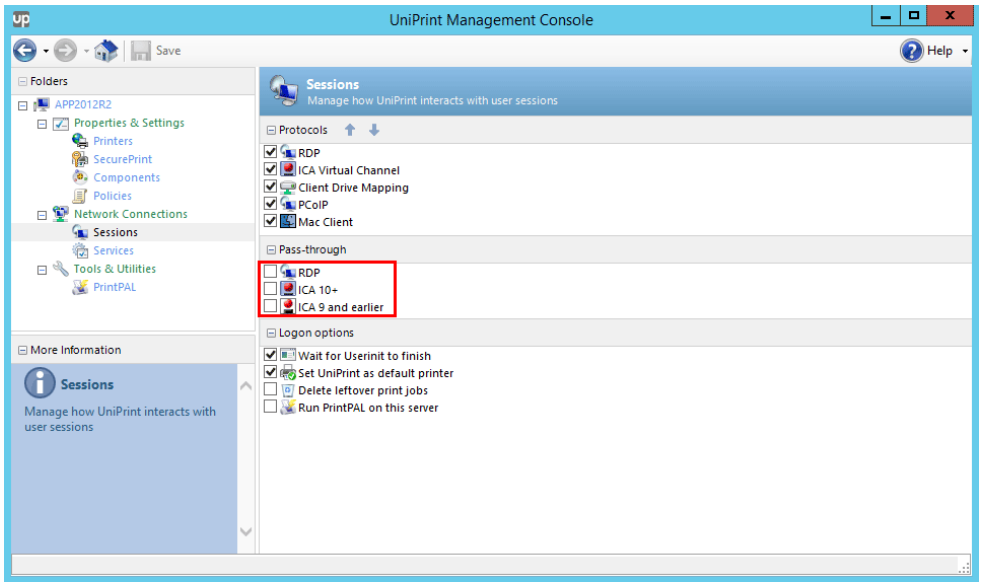
To configure this Application Server to act as a pass-through client, do the following:

1. On the UniPrint Application Server, open the **UniPrint Management Console**.

2. Under **Network Connections**, click **Sessions**.



3. Click to select the protocols that user's use to connect to this Application Server.



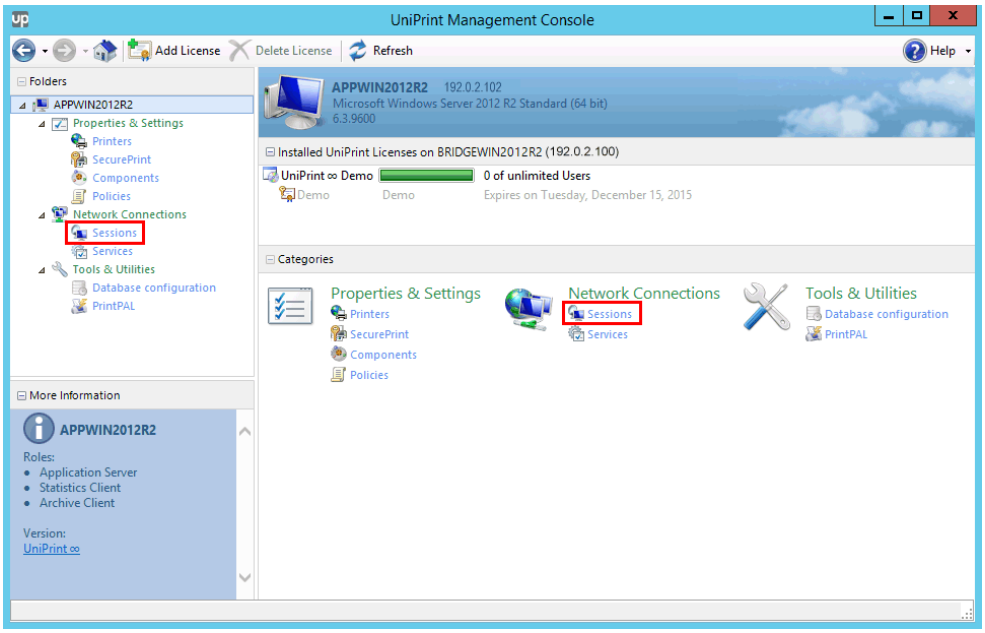
4. Click **Save**.

Setting Session Logon Features

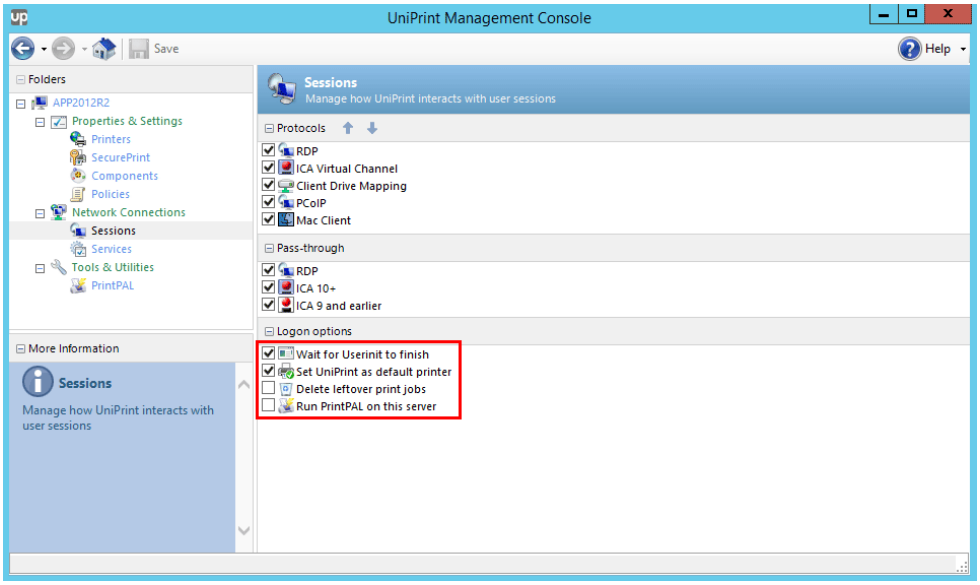
To select which actions are performed when a user launches a session, do the following:

1. On the UniPrint Application Server, open the **UniPrint Management Console**.

2. Under **Network Connections**, click **Sessions**.



3. Click to select the actions you want performed when a session is initiated.



Option	Description
Wait for Userinit to finish	Instructs UniPrint Infinity to wait for Userinit Logon Application to finish before UniPrint UPSession is executed.

Option	Description
Set UniPrint as default printer	All users will have UniPrint set as their default printer in their sessions. Disable this option if UniPrint Client is not deployed.
Delete leftover print jobs	Deletes any leftover print jobs from disconnected sessions when the same user logs back on to this Application Server.
Run PrintPAL on this server	Enables users to add printers by right-clicking the UniPrint icon in the notification area when a session is started and maps printers on behalf of the user.

4. Click **Save**.

Configuring UniPrint Adobe Plug-in

At times re-rendering a document that is already in PDF format may produce undesirable results. In such cases, users can utilize the UniPrint Adobe Plug-in tool to prevent the UniPrint printer driver from re-rendering the file.

If Adobe Reader or Acrobat are already installed, the UniPrint Adobe Plug-in is installed by default when you install the UniPrint Application Server component. The Adobe Plug-in is compatible with Adobe Acrobat or Adobe Reader 5.0 or later.

Replacing the Print function with Print to UniPrint

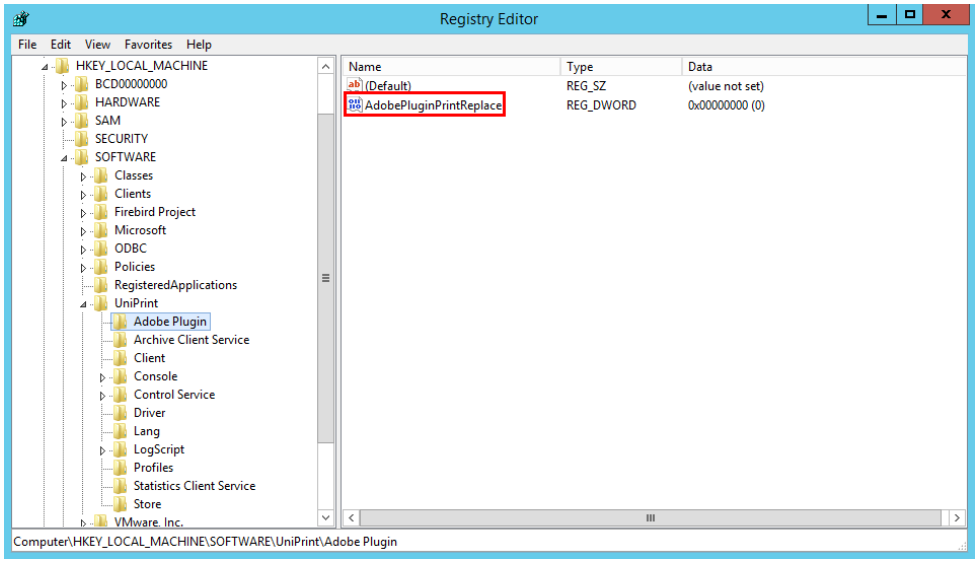
By default, a PDF document will be re-rendered by the UniPrint printer driver if users select **Print** instead of **Print to UniPrint** in the **File** menu. UniPrint Infinity provides a registry key that will change this functionality so that all printing through Adobe Reader/Acrobat will be sent through the UniPrint Adobe Plug-in.

To prevent re-rendering of PDF documents, do the following:

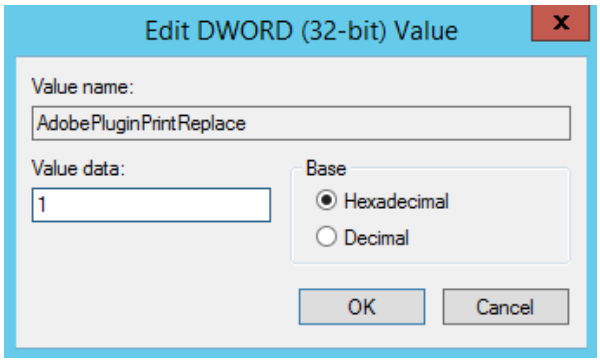
1. On the UniPrint Application Server, click **Start** and then type `regedit`.

2. Under **Search**, click **regedit** to edit the registry.

3. In the registry editor, expand the **HKEY_LOCAL_MACHINE\SOFTWARE\UniPrint\Adobe Plugin** key and double-click **AdobePluginPrintReplace.**



4. Under **Value data**, enter `1` and then click **OK**.



5. Exit the registry editor.

Enabling the UniPrint Adobe Plug-in to run with Adobe Reader XI & Later

Adobe Reader XI and later contains additional security features that hinders the UniPrint Adobe Plug-in from functioning properly. There are two possible workarounds to bypass this issue - the UniPrint Adobe Plug-in can be whitelisted or on a global scale, Protected Mode can be disabled in Adobe Reader at startup.

Whitelisting the UniPrint Adobe Plug-in

To whitelist the UniPrint Adobe Plug-in, do the following:

1. On the UniPrint Application Server with administrative rights, navigate to the UniPrint Infinity installation folder, **\\UniPrint-Infinity-x64-v91\Admin\Adobe Protected Mode**.

2. Copy **ProtectedModeWhitelistConfig.txt**. and paste it into the Adobe Reader installation folder, for example, `C:\Program Files (x86)\Adobe\Adobe Reader DC\Reader`.

3. Ensure that **AcroRd32.exe** also exists in this folder.

4. If **ProtectedModeWhitelistConfig.txt** already exists then copy the contents of the new file into the existing file.

5. In the UniPrint Infinity installation folder, double-click **Enable_whitelist_Reader*.reg**.

6. Click **Yes** to edit the registry.

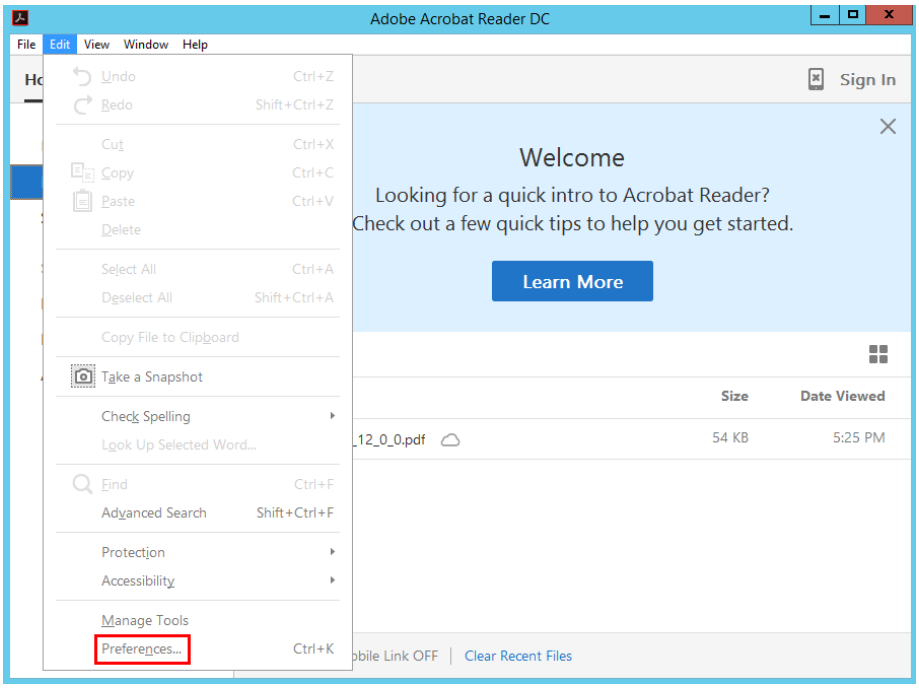
7. Click **OK** to clear the confirmation message.

Disabling Protected Mode at Startup in Adobe Reader XI & Later

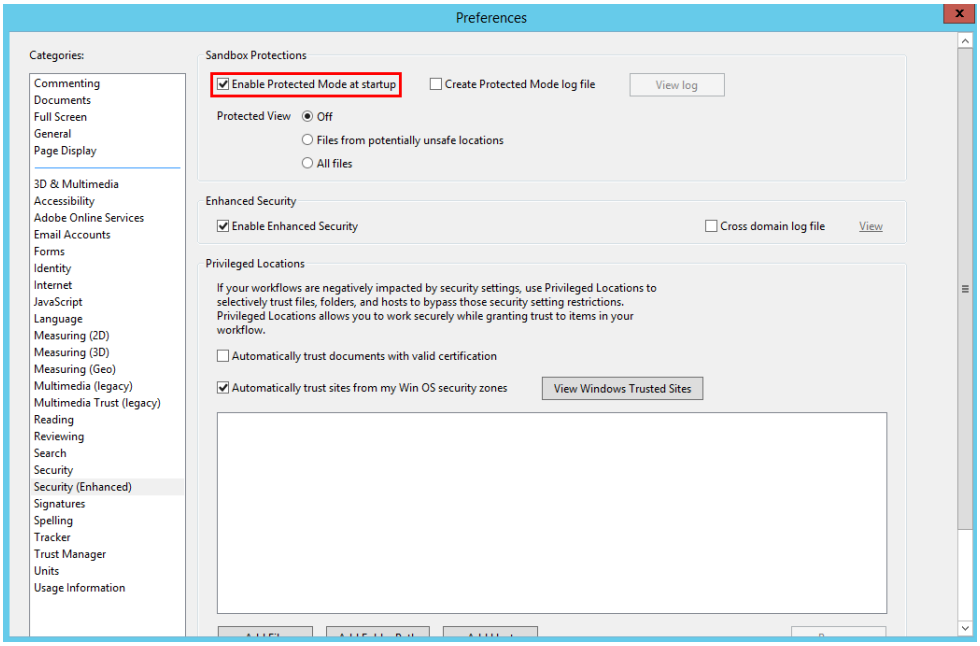
With Adobe Reader XI and later, Protected Mode can be disabled at startup. This feature prevents UniPrint Infinity from reading printer settings. The following steps show how to do this in Acrobat Reader DC.

1. On the UniPrint Application Server, launch Acrobat Reader DC.

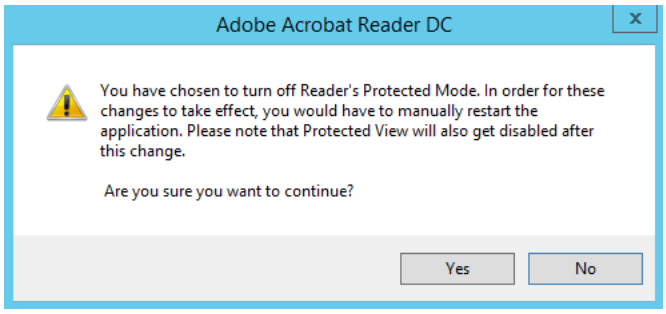
2. In the **Edit** menu, click **Preferences**.



3. Under **Categories**, click **Security (Enhanced)** and then clear **Enable Protected Mode at startup**.



4. Click **Yes**.



5. Click **OK** and then restart Adobe Reader XI or Acrobat Reader DC manually.

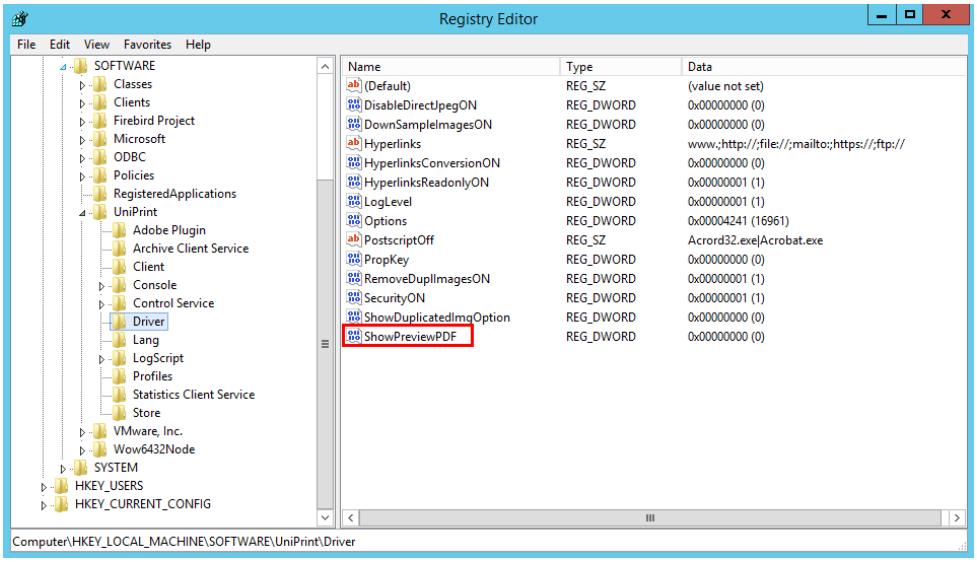
Previewing PDF Documents With Adobe Reader

Some applications do not allow the user to preview their document prior to printing. Zero-client and thin-client users who cannot install the UniPrint Client their on hard drives, can still preview their documents with Adobe Reader through the Application Server.

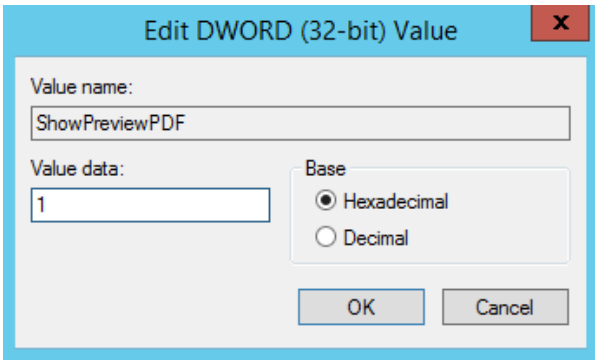
To enable print preview through Adobe Reader on a job-by-job basis, do the following:

1. On the UniPrint Application Server, click **Start** and then type `regedit` to edit the registry.

2. In the Registry Editor, expand **HKEY_LOCAL_MACHINE\SOFTWARE\UniPrint\Driver** and double-click **ShowPreviewPDF**.



3. Under **Value data**, enter `1` and then click **OK**.



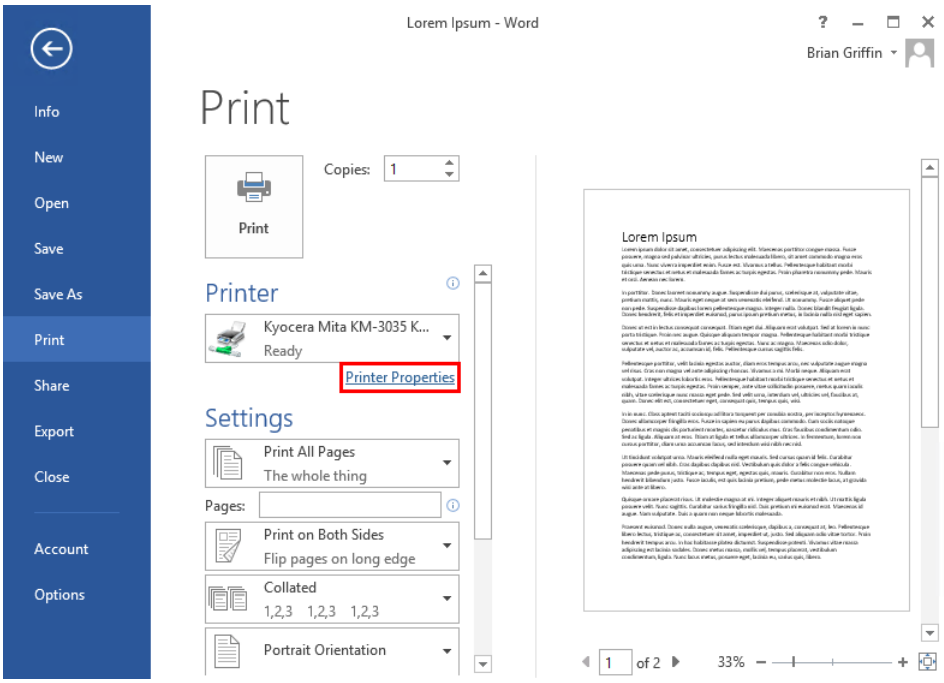
4. Close the registry editor.

Using Adobe Reader to Preview PDF Print Jobs

1. Start a session by logging onto your application server and then open an application, for example Microsoft Word.

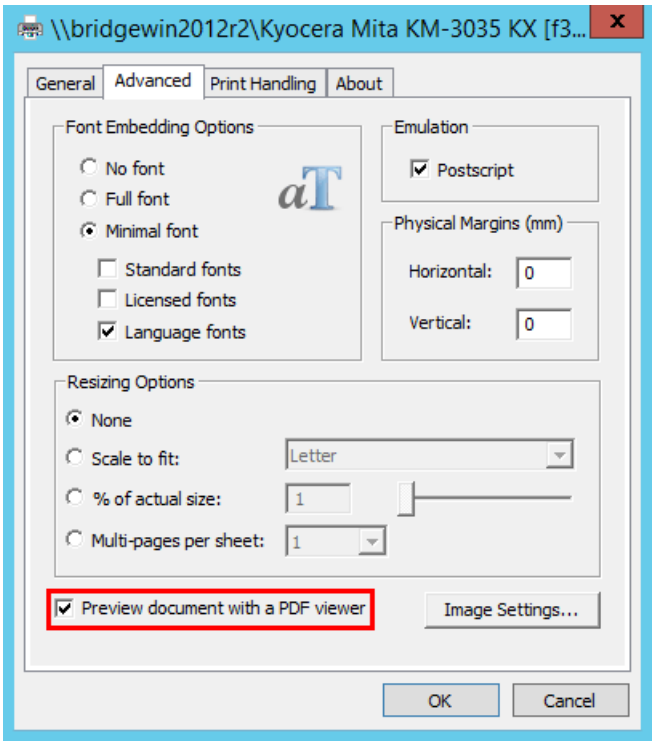
2. Print from the application and select either UniPrint or any Gateway printer.

3. Click **Printer Properties**.



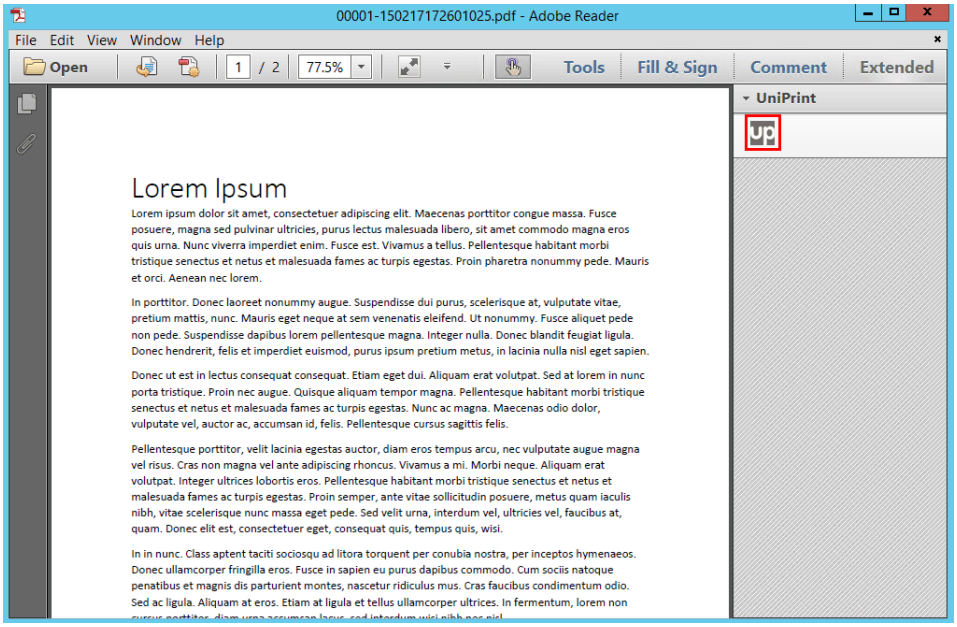
4. Click the **Advanced** tab.

5. Select **Preview document with a PDF viewer** and then click **OK**.



6. Click **Print**.

7. To print from Adobe Reader, click **Extended** and then expand **UniPrint**. Click .



NOTE: In the event of an update of Adobe Reader, the UniPrint Adobe Plug-in (UPPlugin.api) should be copied to %ProgramFiles%\Adobe\...\Reader\plug_ins. For Adobe Acrobat, copy the UniPrint Adobe Plug-in (UPPlugin.api) to %ProgramFiles%\Adobe\...\Acrobat\plug_ins.

Creating Multiple UniPrint Printer Queues

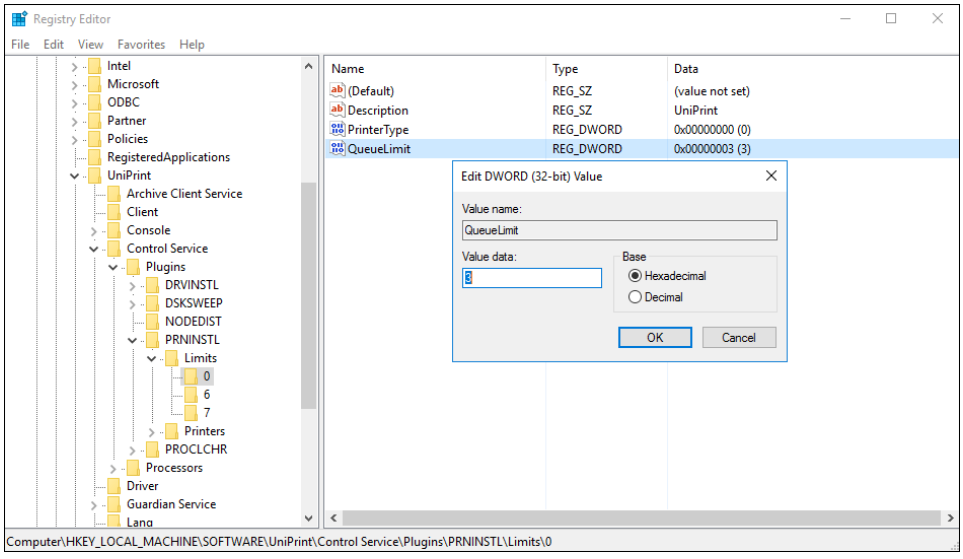
At times it may be necessary to create multiple UniPrint printer queues on the Application Server. Multiple queues are typically used for Print Route (Smart Route) and for multiple queue mappings with UniPrint Client.

Changing the Number of Allowable UniPrint Queues

The default number of UniPrint queues is three for the UniPrint, UniPrint (Email PDF) and UniPrint (Save PDF) queues. In order to increase the number of allowable UniPrint queues, do the following:

1. On the Application Server, open the **Registry Editor** by clicking **Start** and then typing **`Regedit`**.

2. Under the following key: **HKEY_LOCAL_MACHINE \SOFTWARE\UniPrint\Control Service\Plugins \PRNINSTL\Limits\0**, right-click **QueueLimit** and then select **Modify**.



3. Edit the **QueueLimit** and then click **OK**.

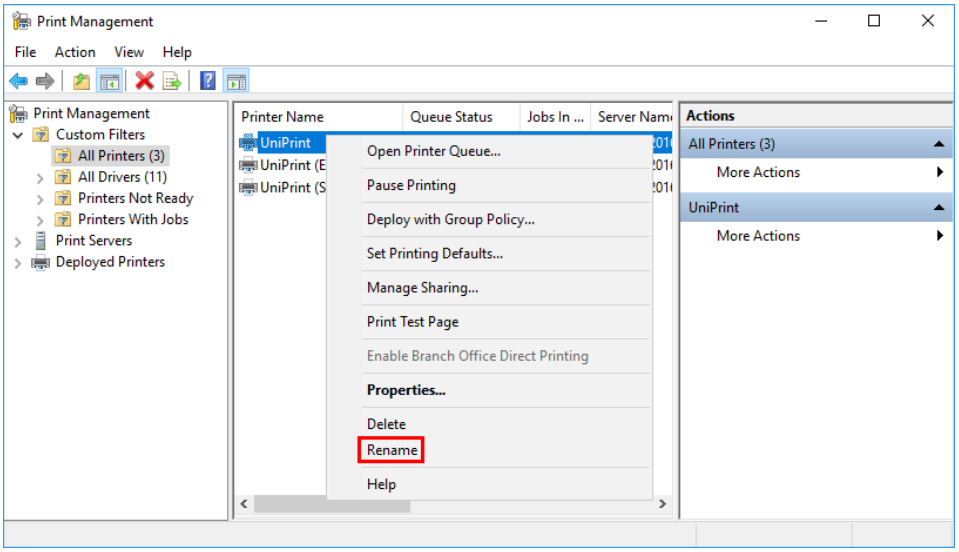
Creating Another UniPrint Printer Queue

To create another UniPrint printer queue, do the following:

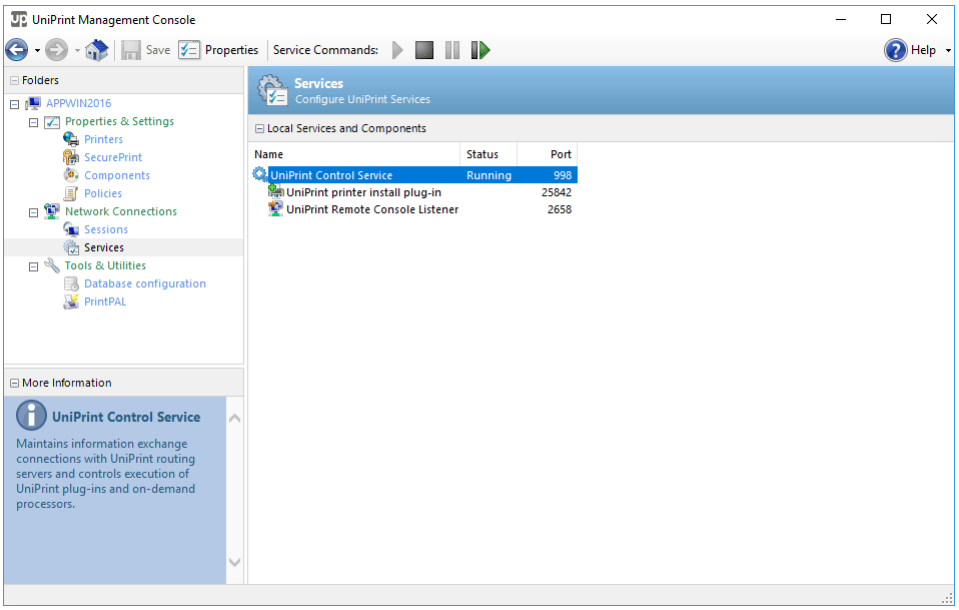
1. On the Application Server, open **Print Management**.

2. Under **Custom Filters**, click **All Printers**.

3. Right-click **UniPrint** and then select **Rename**. Give the UniPrint printer a different name.

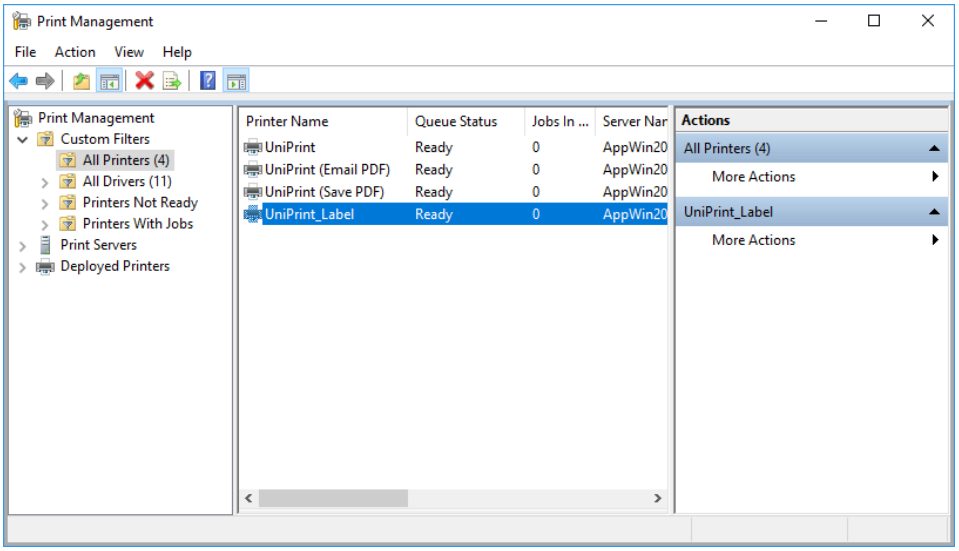


4. In the **UniPrint Management Console**, under **Network Connections**, click **Services**.



5. Click to select the **UniPrint Control Service** and then click to restart the service.

6. In **Print Management**, a new **UniPrint** queue will be created.



7. To create more UniPrint queues, continue renaming the UniPrint queue and then restarting the UniPrint Control Service.

CHAPTER 6

UniPrint Infinity

Configuring UniPrint Using ADMs & ADMXs

Most configuration can be done through the UniPrint Management Console, however, UniPrint has provided administrative templates to standardize configuration for a larger number of users and endpoint devices.

ADM, ADMX and ADML (Administrative Template) files are available in the UniPrint Infinity installation package in the **Admin** folder. Using an administrative template file, network administrators can configure default UniPrint settings in a structured manner for all users.

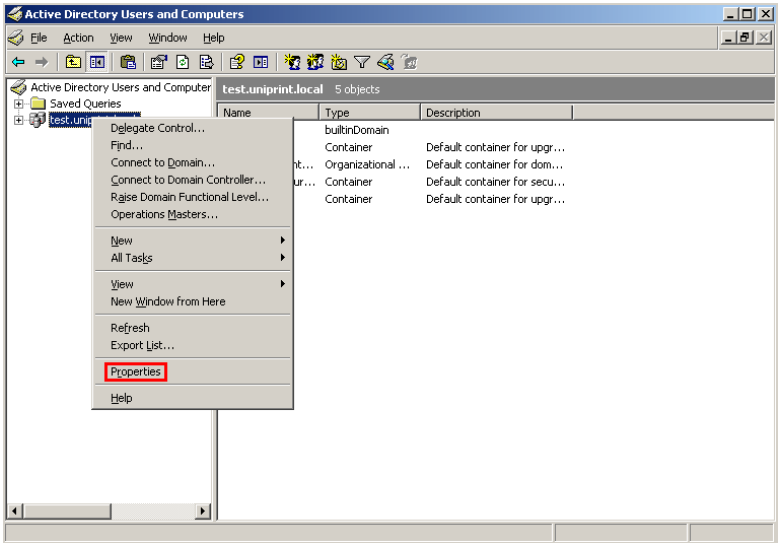
Loading a Classic Administrative Template

The following instructions are based on Windows Server 2003. For other versions of Windows, refer to your Microsoft documentation. Before proceeding, copy UniPrint9_Services.adm to a distribution point that is accessible by the domain controller.

To load the classic administrative template, **UniPrint9_Services.adm,** into Group Policy Object Editor:

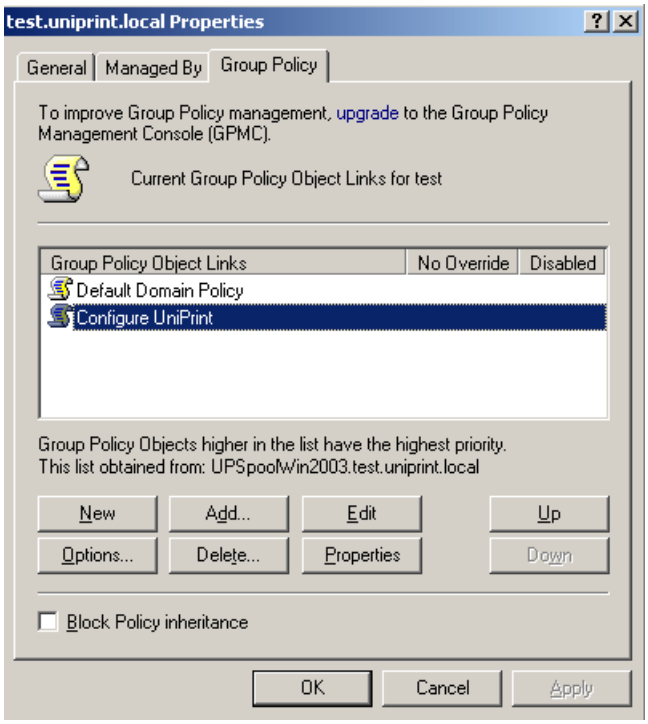
1. From your domain controller, click **Start**, point to **Programs**, **Administrative Tools** and then click **Active Directory Users and Computers**.

2. Right-click the domain that you want **UniPrint9_Services.adm** to be applied to and then select **Properties**.

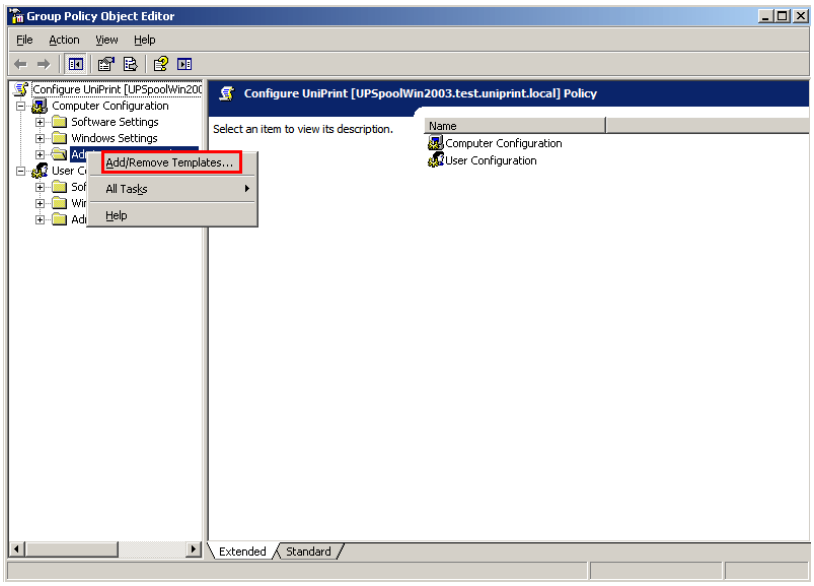


3. Click the **Group Policy** tab.

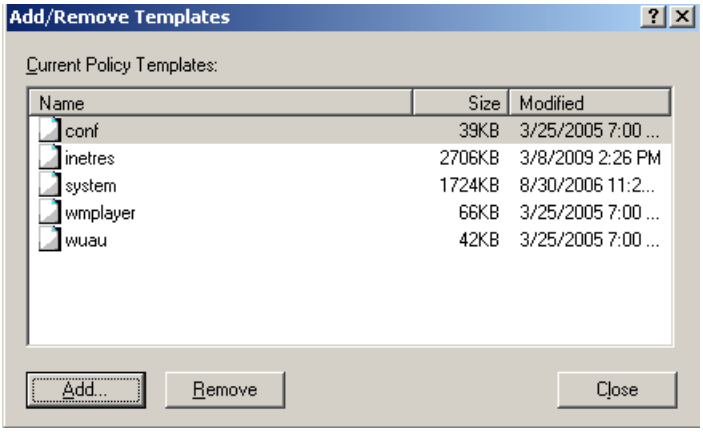
4. Select the Group Policy setting you want to edit and then click **Edit** to open the **Group Policy Object Editor**.



5. Under either **Computer Configuration** or **User Configuration**, right-click **Administrative Templates** and then select **Add/ Remove Templates**.



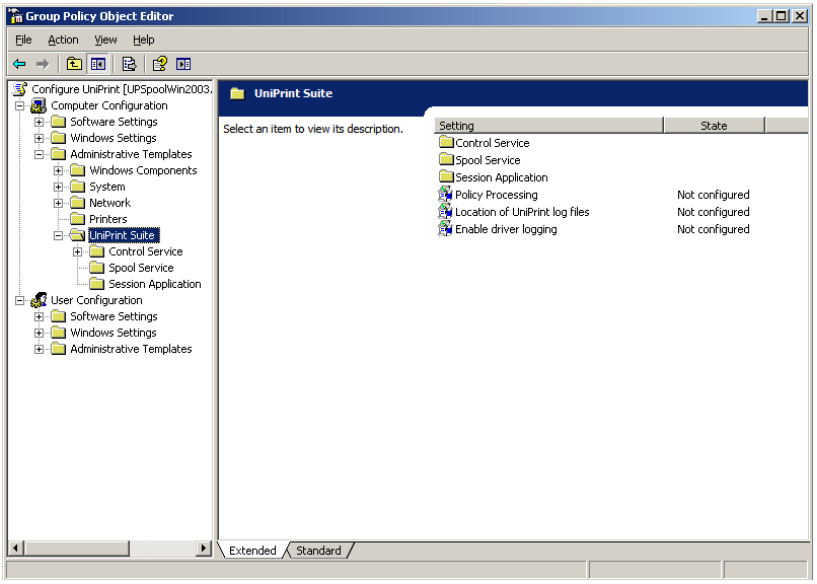
6. Click **Add.**



7. Browse to the location where **UniPrint9_Services.adm** is stored and then click **Open** to add the new template.

8. Click **Close**.

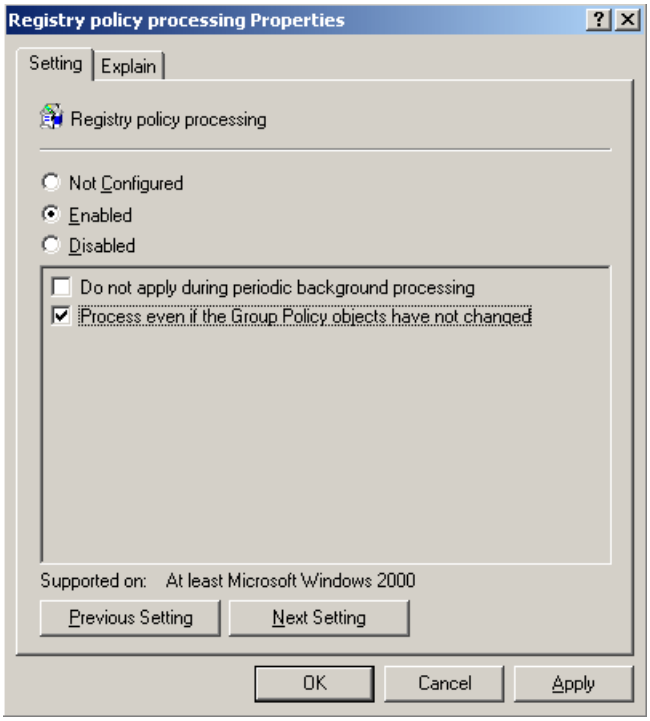
9. Settings are divided into several categories and by default are **Not configured**.



10. To edit any of these settings, double-click the setting and select **Enabled**. For more information on each setting, click the **Explain** tab.

11. To ensure that the ADM settings are set on the domain controller, expand **Computer Configuration**, **Administrative Templates**, **System**, and **Group Policy**.

12. Double-click on **Registry policy processing** and select **Enabled**. Select **Process even if Group Policy objects have not changed** and then click **OK**.



13. Close the Group Policy Object Editor and click **OK** to return to Active Directory Users and Computers.

Loading and Configuring an Administrative Template in Windows Vista or later

Windows Vista, Windows 7, Windows Server 2008 and later support XML-based ADM files, ADMX and ADML. ADML are XML-based ADM files that contain language-specific settings. Unlike, ADM files, ADMX files are not stored in individual Group Policy Objects and do not need to be "loaded", only copied to the appropriate folders.

The following instructions are based on Windows Server 2012 R2. For other versions of Windows, refer to your Microsoft documentation.

1. Copy **UniPrint9_Services.admx** from the UniPrint Infinity installation package **Templates** folder to either the central store on the domain controller, *FQDN*\SYSVOL*FQDN*\Policies \PolicyDefinitions or to the local store, %systemroot%\ PolicyDefinitions, where *FQDN* is the fully qualified domain name.

2. Copy **UniPrint9_Services.adml** from the UniPrint Infinity installation package Templates folder to either the central store on the domain controller, *FQDN*\SYSVOL*FQDN*\Policies\PolicyDefinitions\en-US or to the local store, %systemroot%\PolicyDefinitions\en-US, where *FQDN* is the fully qualified domain name.

NOTE: In Windows Server 2008 or later, the **Group Policy Management** feature must be enabled first. To enable Group Policy Management, do the following:

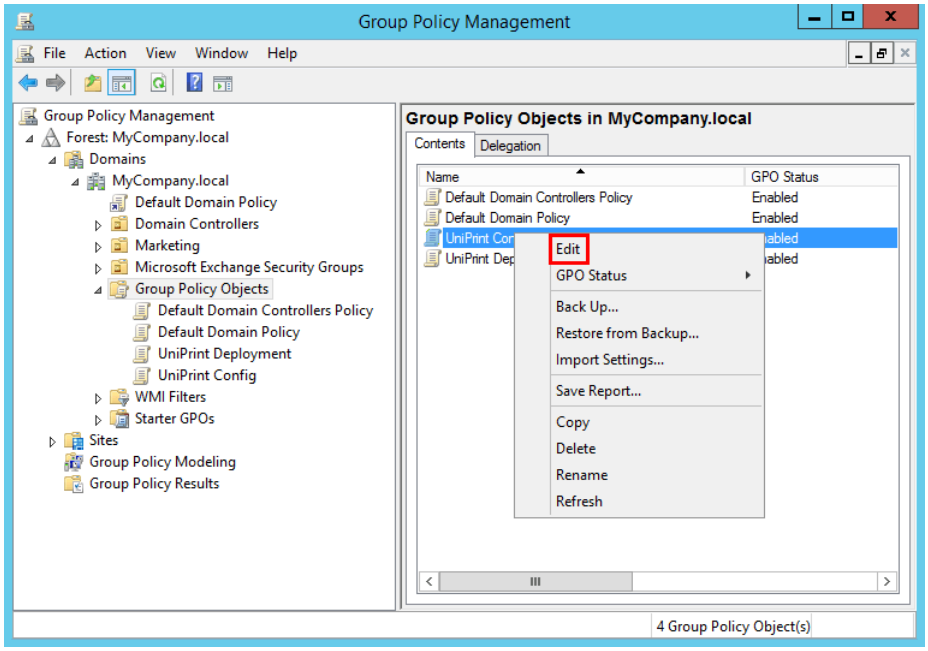
1. From the desktop, click **Start** and then click **Server Manager**.
2. In **Server Manager**, click **Add roles and features**.
3. Follow the steps in the **Add roles and features** wizard until you get to the **Features** dialog box.
4. From the list of available features, click to select **Group Policy Management** and then click **Install**.
5. Continue through the wizard until complete.

6. From your domain controller, click **Start** and then type **Group Policy Management**.

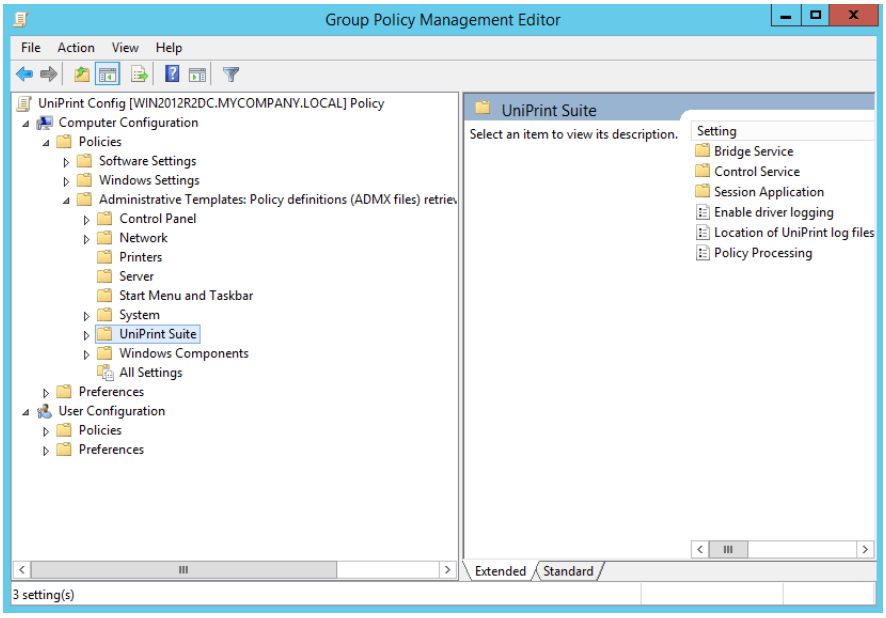
7. Under **Search**, double-click **Group Policy Management.**

8. Expand your domain and then click **Group Policy Objects**.

9. Right-click the Group Policy Object that you want to edit and then click **Edit** to open the **Group Policy Object Editor**.



10. Expand either **Computer Configuration** or **User Configuration**, **Policies**, **Administrative Templates**, and then click **UniPrint Suite**.



11. Settings are divided into several categories and by default are **Not Configured**. To modify a setting, double-click the setting and select **Enabled**. For more information on the setting, click the **Explain** tab.

CHAPTER 7

UniPrint Infinity

Configuring PrintPAL

PrintPAL is a proximity-based printing utility that can be used to eliminate the need to create and compile Windows scripts. When a user logs onto a session, PrintPAL will automatically map selected printers to their session.

Configuring PrintPAL involves four major steps:
1. Planning out a PrintPAL map
2. Creating a PrintPAL map
3. Testing the PrintPAL map
4. Setting PrintPAL to automatically map printers on the Application Server.

The majority of the configuration time involves creating a PrintPAL map, so we recommend first planning out your device-to-printer map, otherwise known as a PrintPAL map.

NOTE: Ensure that the **PrintPAL Server** component is installed on the UniPrint Bridge and that the **Run PrintPAL on this server** option is enabled on all UniPrint Application Servers.

Planning Your PrintPAL Mapping

Planning your PrintPAL mapping can save you hours of troubleshooting. You can plan for the majority of your PrintPAL map by examining your network topology, client devices on your network and how you want to group the client devices with UniPrint Gateway printers on your network.

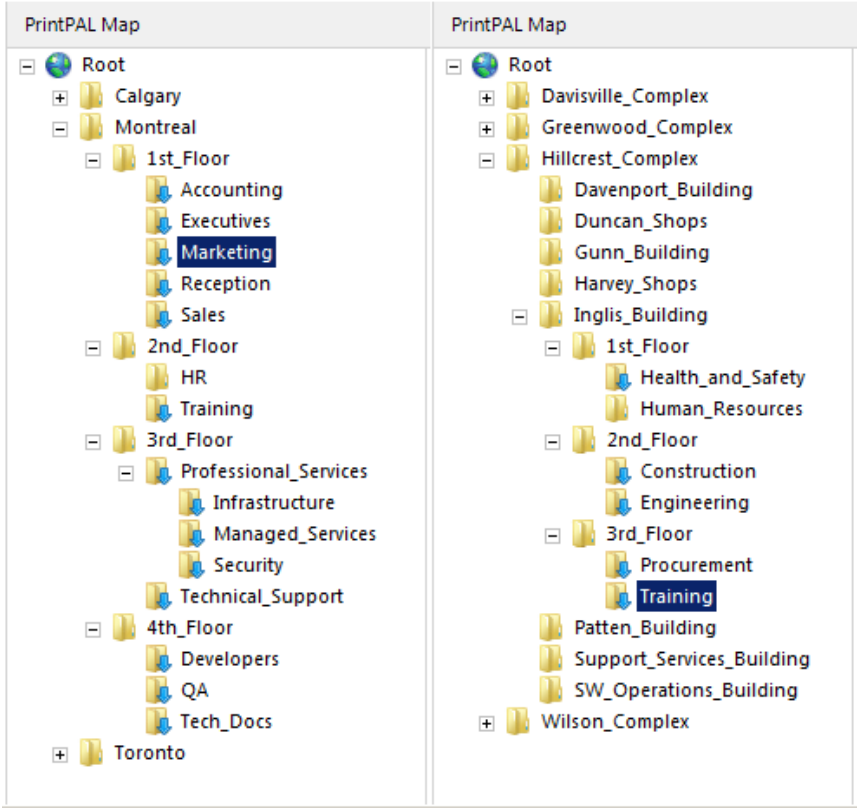
Grouping clients devices may depend on your organizational structure, corporate security policies and network environment. Other parameters to consider are the following:

- Geographic location (country, province/state, city)
- Complex or campus
- Building name
- Floor or level
- Department
- Job function or job title

As the network administrator, you will also have to determine which groups of client devices will initially have access to a set of Gateway printers. This can

be based on the proximity to a printer or it can be based on corporate security policies or a combination of both.

The following are two examples of how to group client devices.



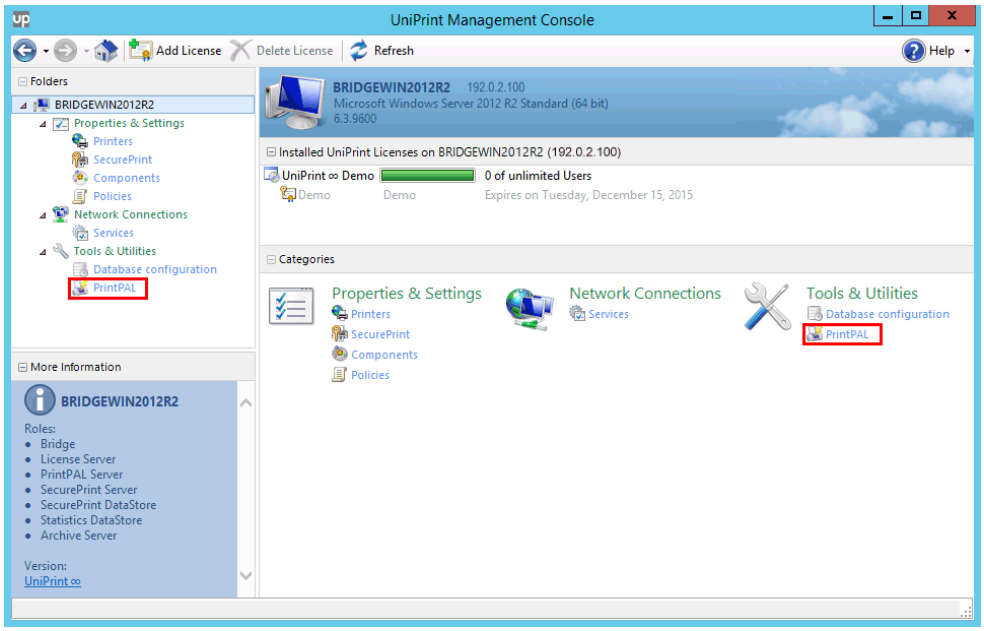
NOTE: For endpoint devices with Windows 10 Build 1511 or later, ensure that automatic default printer management is disabled. This is required in order for PrintPAL mapping to work properly. For more information, see "Disabling Automatic Default Printer Management in Windows 10" on page 14.

Setting Initial PrintPAL Configuration Settings

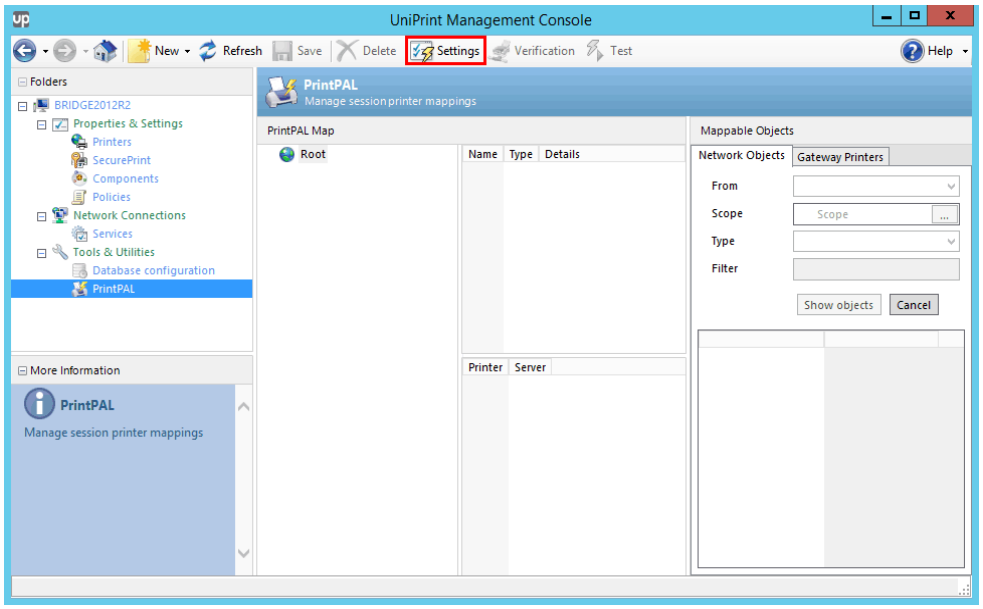
The initial PrintPAL setup must be done from the UniPrint Bridge. Managing PrintPAL can be done from any Application Server however, PrintPAL performs best when managed from the UniPrint Bridge.

1. On the UniPrint Bridge, open the **UniPrint Management Console**.

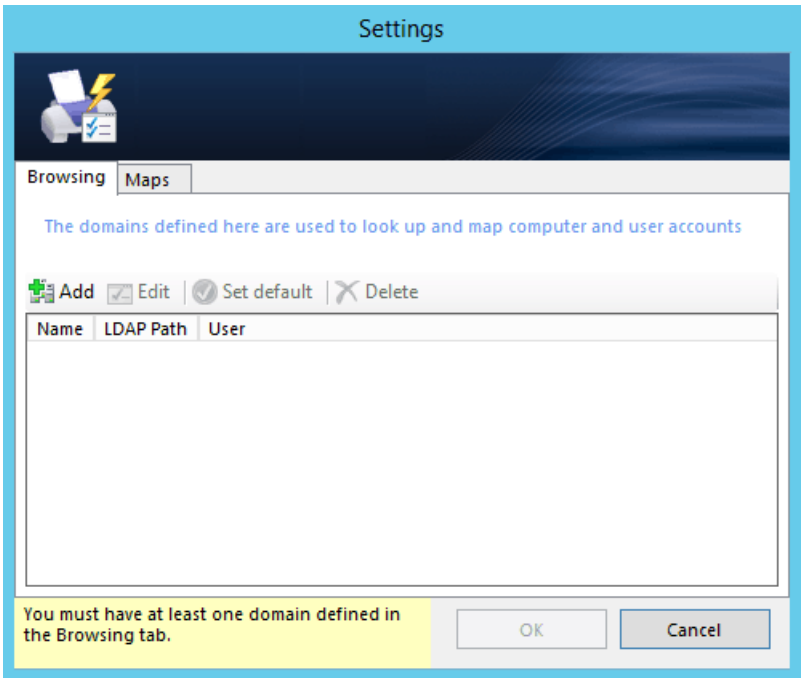
2. Under **Tools & Utilities**, click **PrintPAL**.



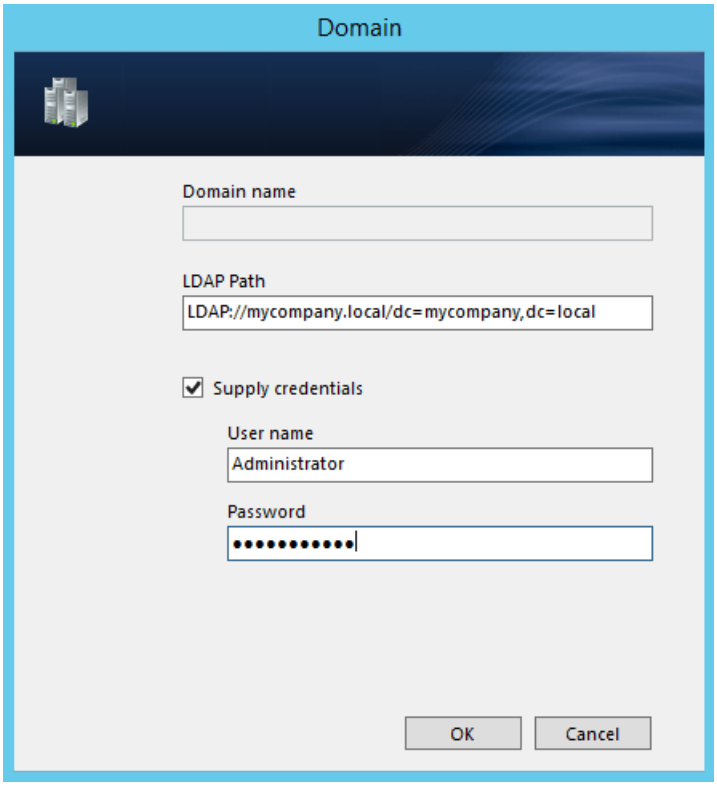
3. Click **Settings**.



4. In the **Browsing** tab, click **Add**.

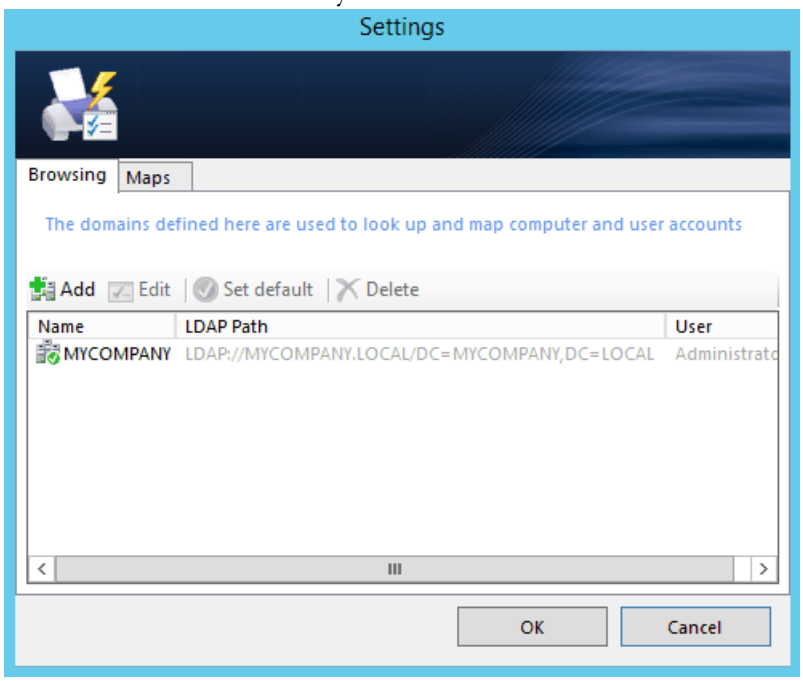


5. In the **Domain** dialog box, under **LDAP path**, enter the URL of your LDAP server.

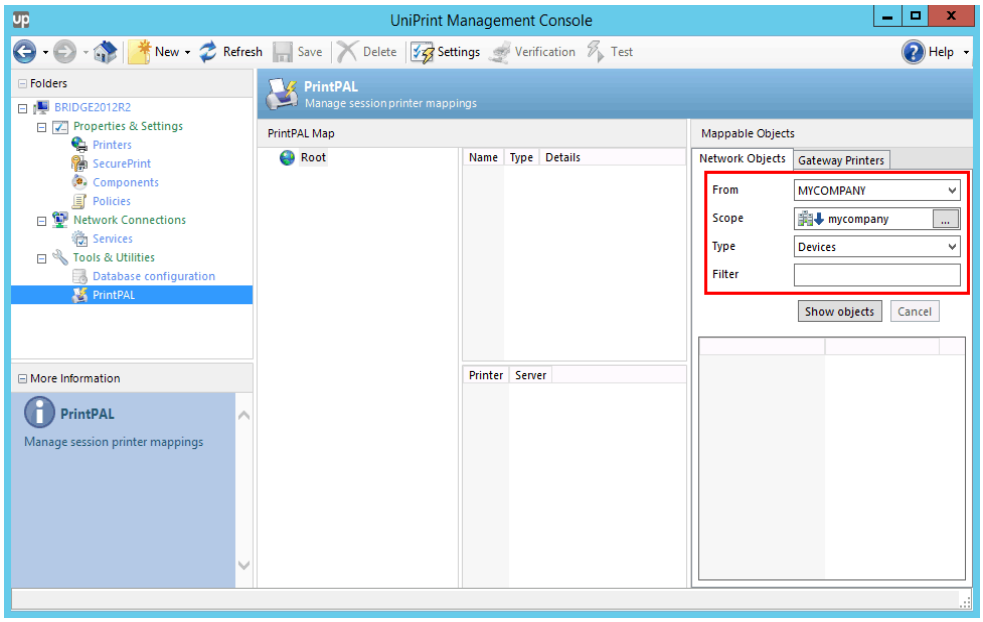


a) If your LDAP server requires authentication, select **Supply credentials** and then type in a **User name** and **Password**. Click **OK**.

6. PrintPAL will connect to your LDAP server. Click **OK**.



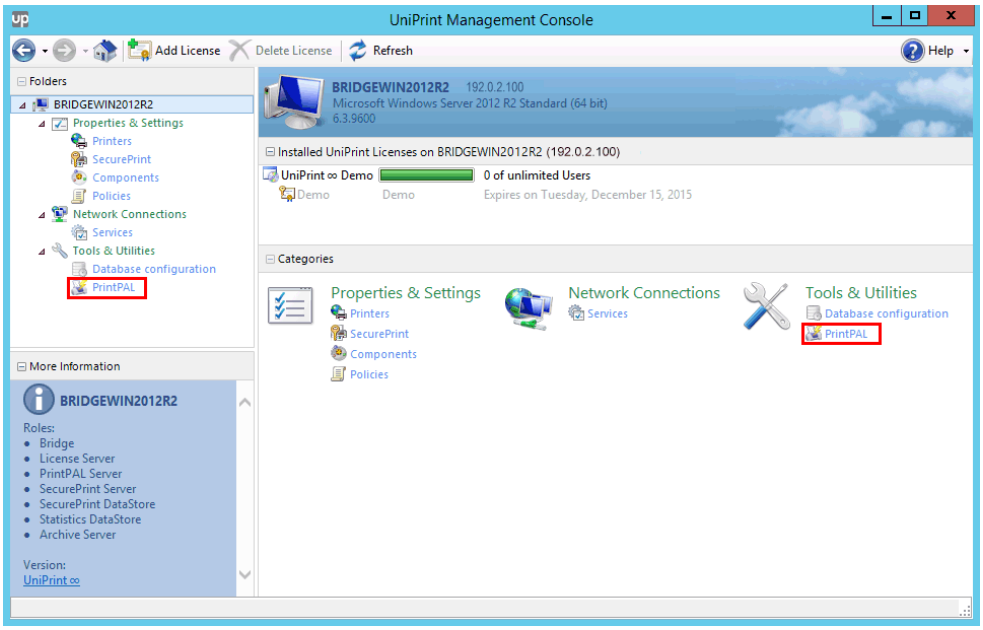
7. The domain will appear on the right side below **Mappable Objects**.



Creating Groups for the PrintPAL Map

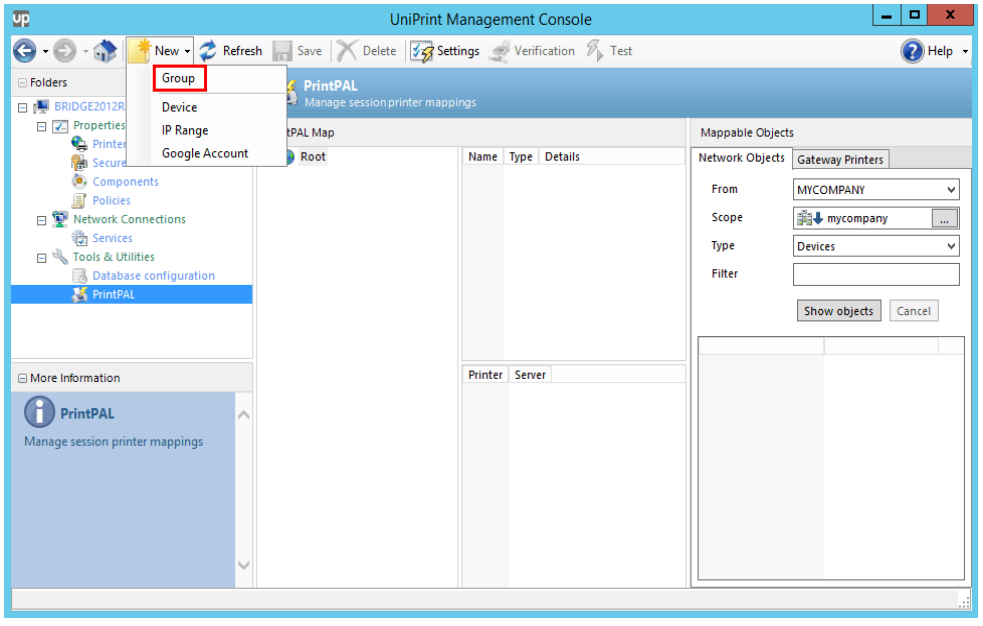
1. On the UniPrint Bridge, open the **UniPrint Management Console**.

2. Under **Tools & Utilities**, click **PrintPAL**.



3. Under **PrintPAL Map**, click to select a parent group. If you are starting with a blank pane, click to select **Root**.

4. Click **New** and then click **Group**.



5. In the **New Group** dialog box, enter the group name. If this group is to inherit devices and printers from the parent group, select the **Inherit printers from parent group**. If all criteria set in the group matches, select **Match all criteria types**, for this group to map printers to a session. For example, if an IP range and a user group are defined in the group, then the device must belong to the IP range AND the user must belong to the user group before printers are mapped to the session. Click **OK**. ***Note***: *spaces and other special characters are not accepted, except the underscore (_).*

6. Repeat steps 3 to 5 to create additional groups.

7. Click **Save** to save your PrintPAL map.

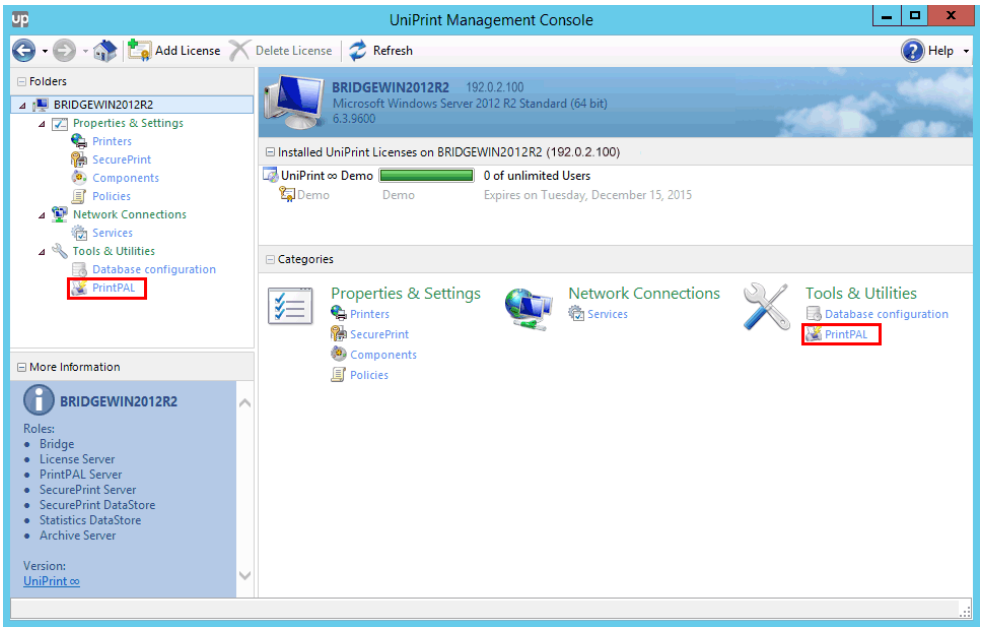
NOTE: indicates that the group has inherited objects and printers from the parent group. indicates that the group does not inherit objects and printers from the parent group. indicates that all criteria defined in the group must match before printers are mapped to a session.

Adding A Device to the PrintPAL Map

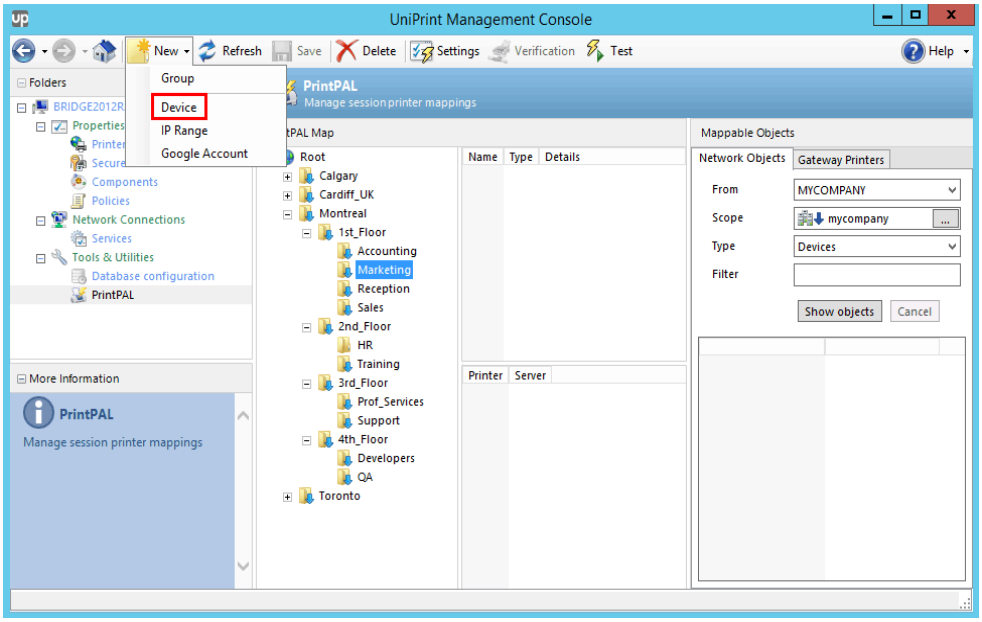
This feature is good for adding devices, such as client endpoints, that do not necessarily belong to a domain. For example, devices that belong to a workgroup.

1. On the UniPrint Bridge, open the **UniPrint Management Console**.

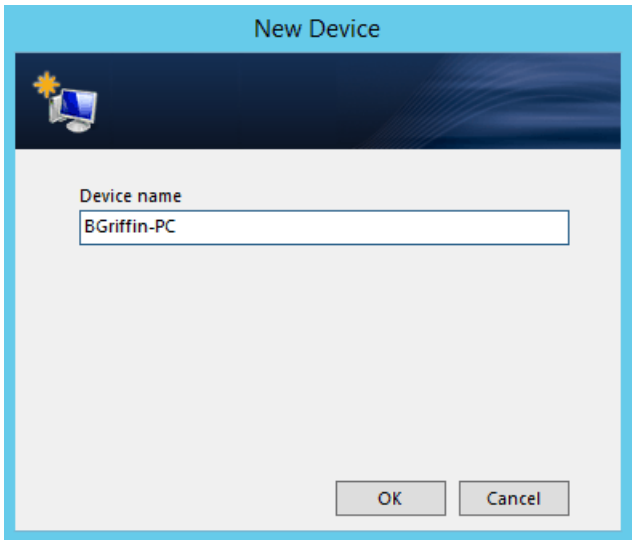
2. Under **Tools & Utilities**, click **PrintPAL**.



3. Under PrintPAL Map, click to select a group, click **New** and then click **Device**.

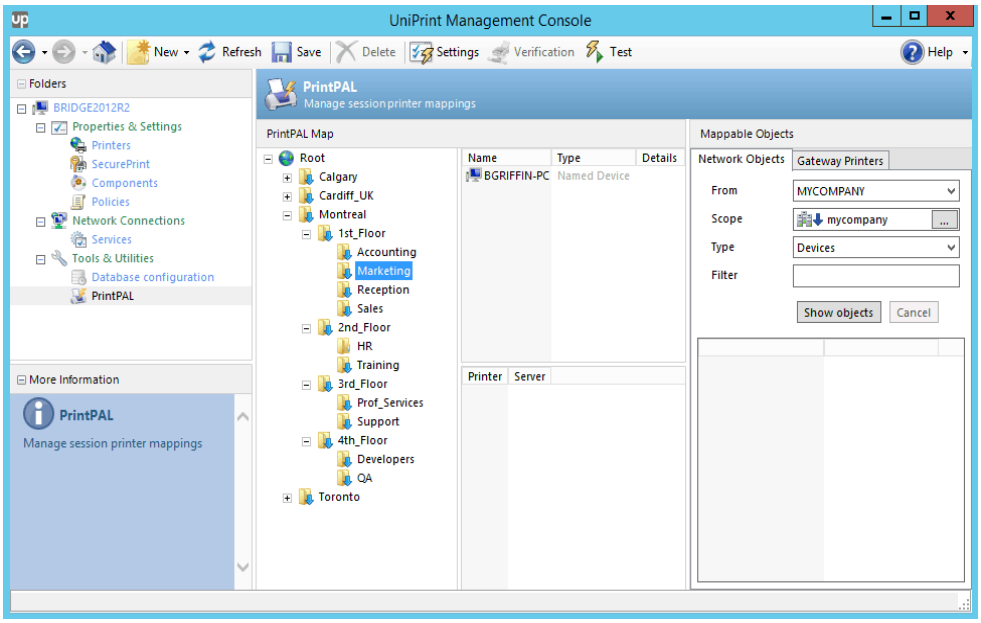


4. In the **New Device** dialog box, type the name of the device and then click **OK**.



5. Repeat steps 3 and 4 to add additional devices.

6. Click **Save** to save your PrintPAL map.

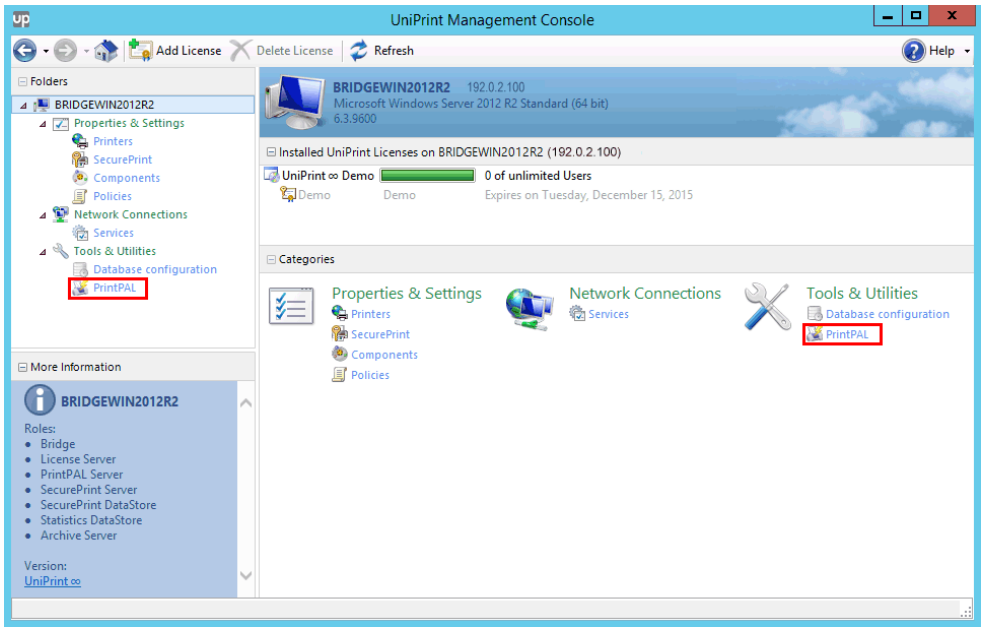


Adding an IP Range of Objects to the PrintPAL Map

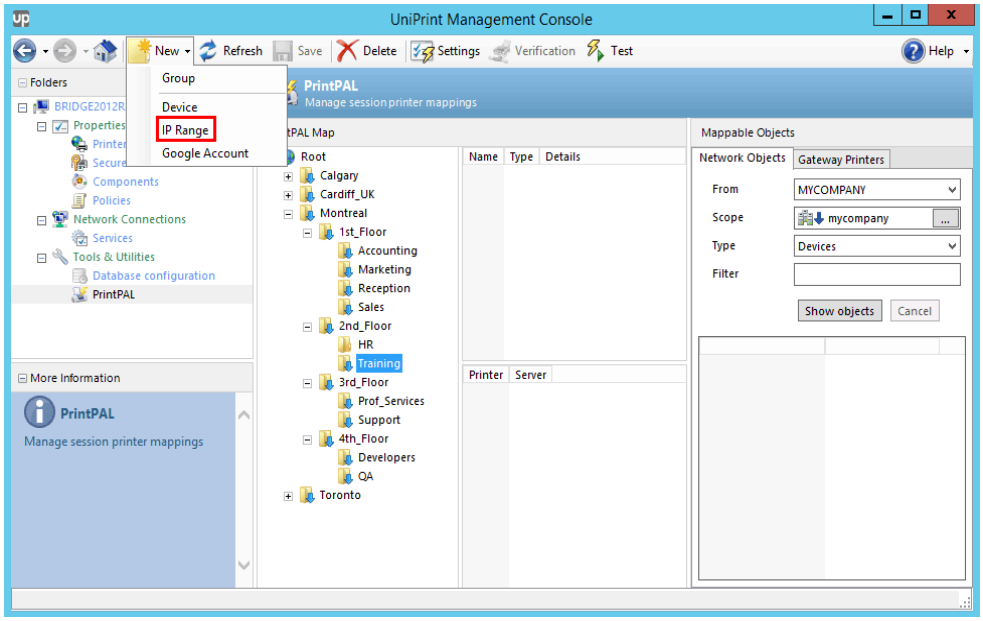
This feature is good for a group of objects that utilize static IP addresses. This feature saves time since the network administrator does not need to go through the list of **Network Objects** individually under **Mappable Objects**, which can be a lengthy process for large environments.

1. On the UniPrint Bridge, open the **UniPrint Management Console**.

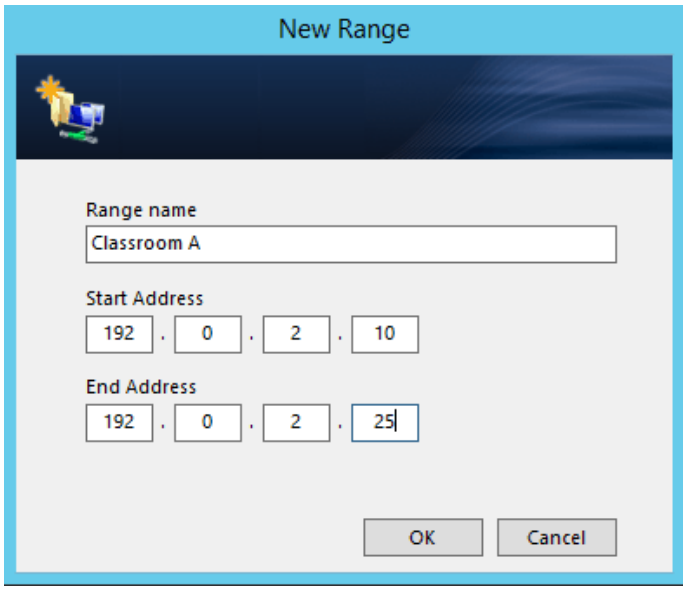
2. Under **Tools & Utilities**, click **PrintPAL**.



3. Under **PrintPAL Map**, click to select a group, click **New** and then click **IP Range**.

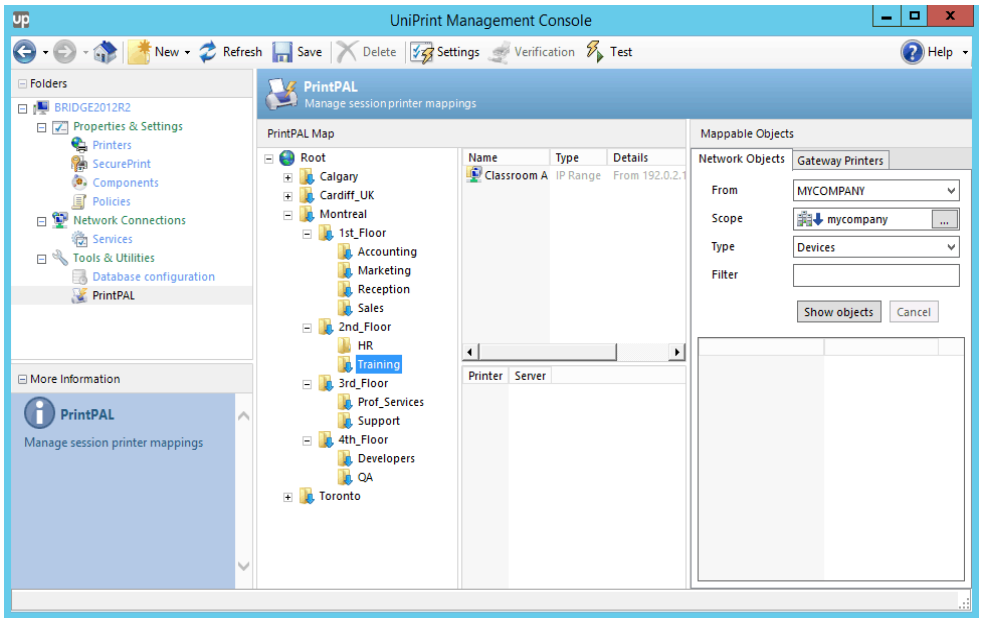


4. In the **New Range** dialog box, enter the **Range name** and the beginning and ending IP addresses. Click **OK**.



5. Repeat steps 3 and 4 to add additional IP ranges.

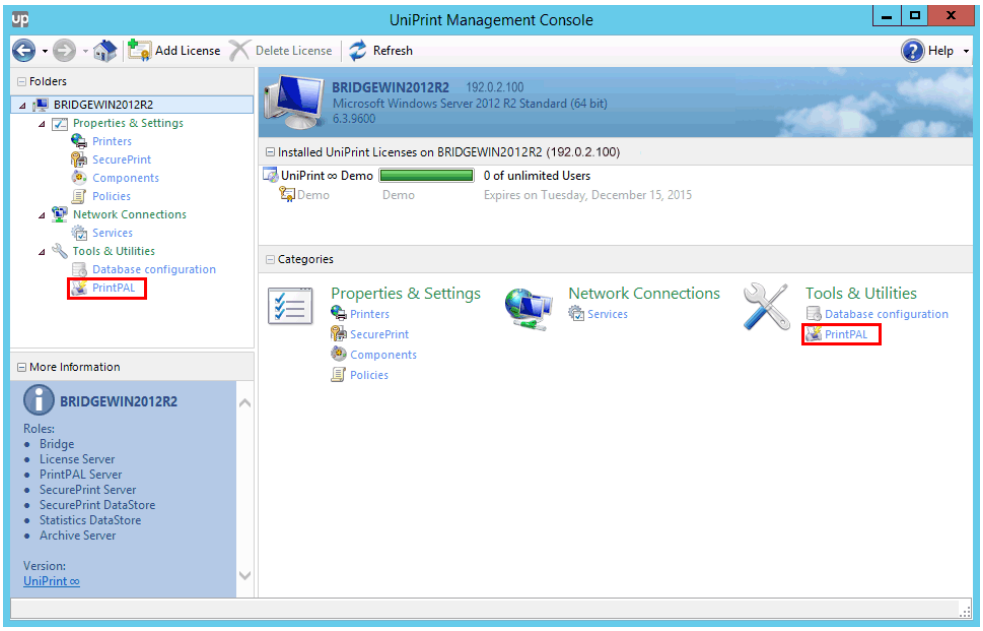
6. Click **Save** to save your PrintPAL map.



Mapping Network Objects to a Group in PrintPAL

1. On the UniPrint Bridge, open the **UniPrint Management Console**.

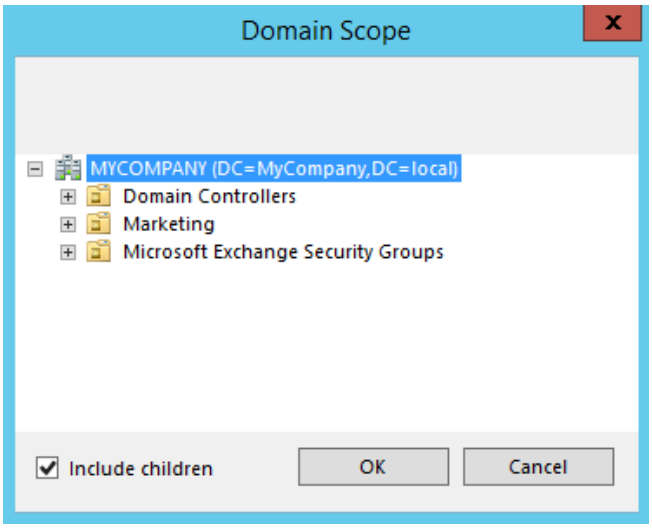
2. Under **Tools & Utilities**, click **PrintPAL**.



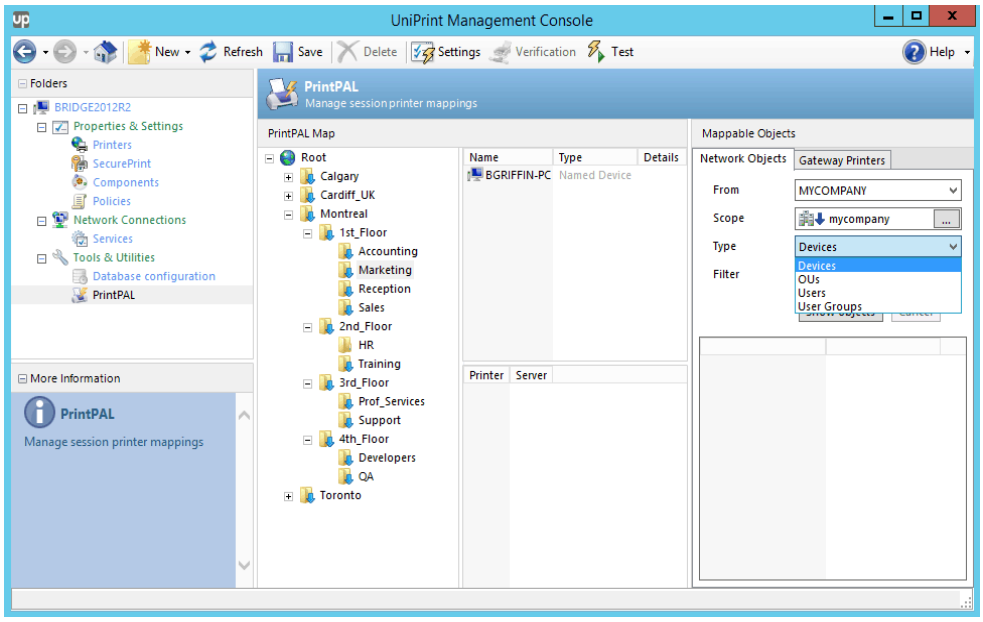
3. Under **PrintPAL Map**, click to select the group to which you want to map objects.

4. If there are multiple domains, in the **Network Objects** tab, from the **From** list, select the domain from which you wish to map.

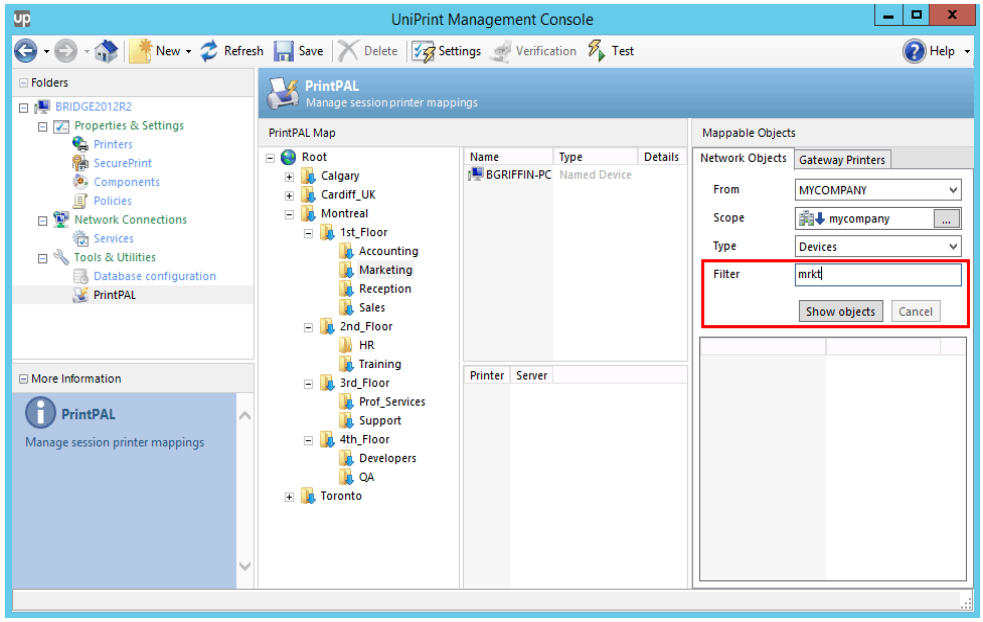
5. Click ... to select a scope of the domain and if children are to be included in the list below. Click **OK**.



6. From the **Type** list, click the type of object you want to map, for example, **Devices**, **OUs**, **Users** or **User Groups**.



a. Beside **Filter**, enter in a character string that you want the list to filter and then click **Show Objects**.

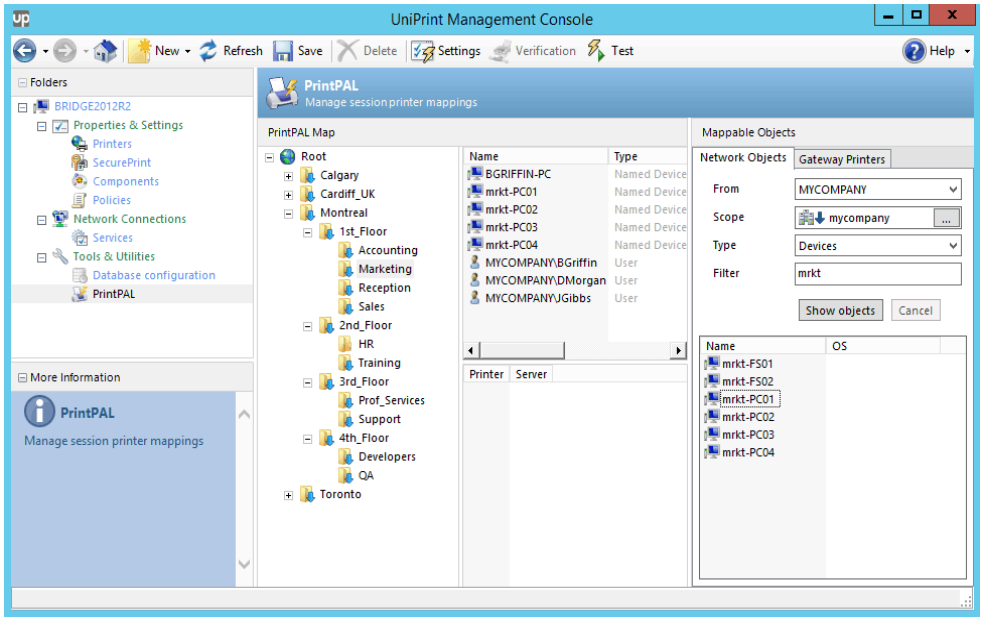


7. Click to select an object and then either double-click it or press **ENTER** to add it to PrintPAL map.

NOTE: To add multiple objects that appear consecutively in the list, click the first object you want to add, press **SHIFT** and then click the last object. Press **ENTER** to add them to the PrintPAL map. To add multiple objects that do not appear consecutively in the list, click to select an object, press **CTRL**, and then click the next object. Press **ENTER** to add the objects to the PrintPAL map.

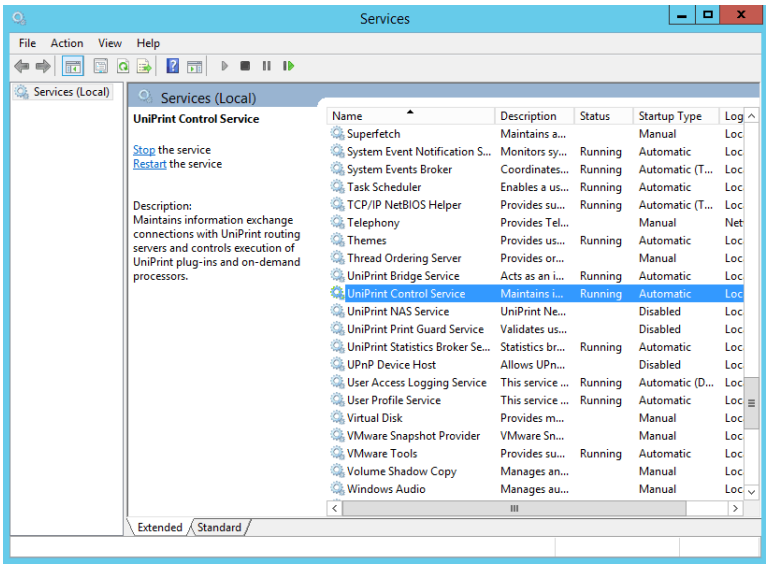
8. Repeat steps 6 and 7, selecting groups and mapping objects to these groups as required.

9. Click **Save** to save your PrintPAL map.

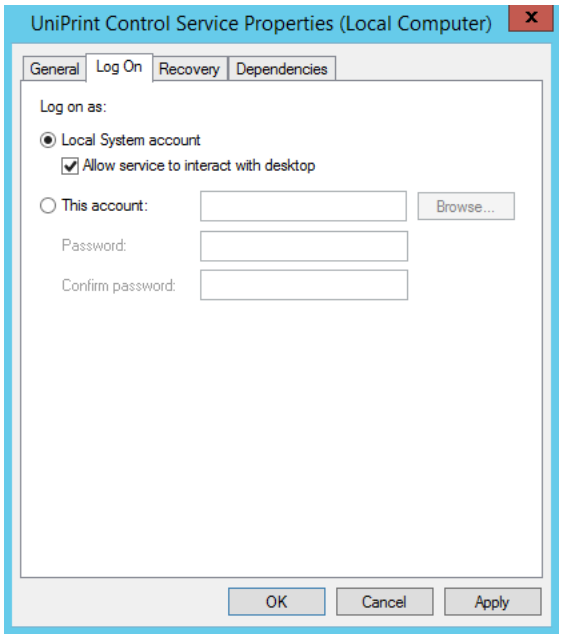


NOTE: In a trusted cross domain environment, in order for object SIDs to be resolved, enable **Allow service to interact with desktop** in the **UniPrint Control Service properties**, by doing the following:

1. Click **Start** and then type `Services`.
2. Under **Search**, double-click **Services**.
3. Double-click **UniPrint Control Service** and then click the **Log On** tab.



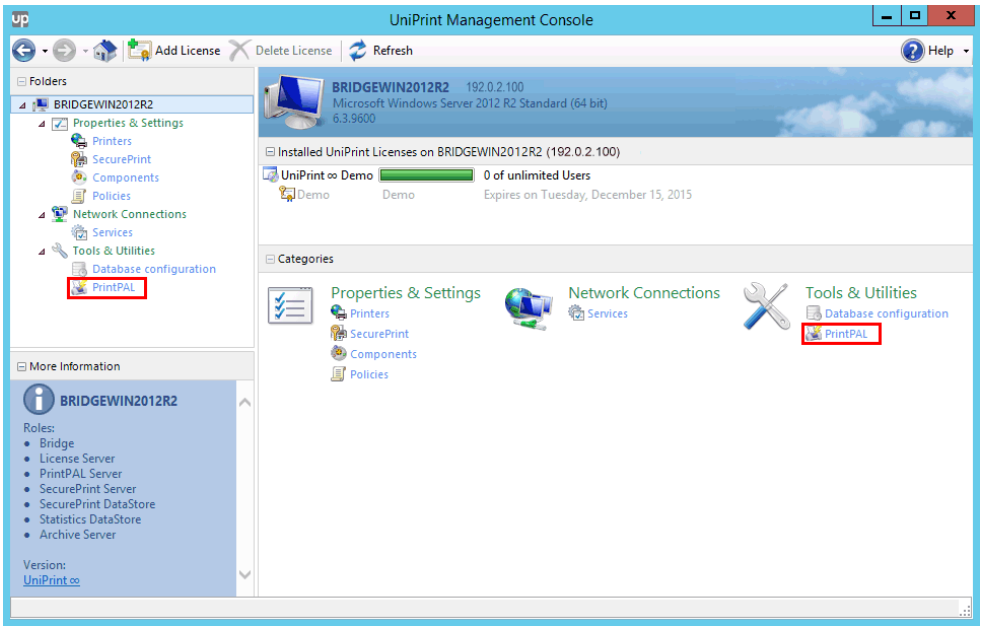
4. Under **Local System account**, select **Allow service to interact with desktop** and then click **OK**.



Mapping Printers to a Group in PrintPAL

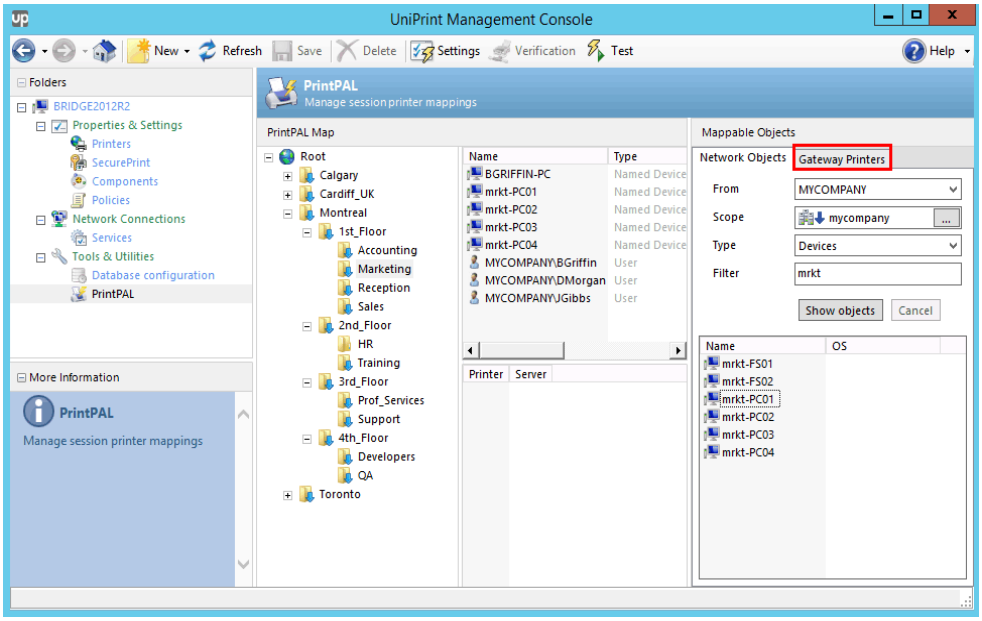
1. On the UniPrint Bridge, open the **UniPrint Management Console**.

2. Under **Tools & Utilities**, click **PrintPAL**.

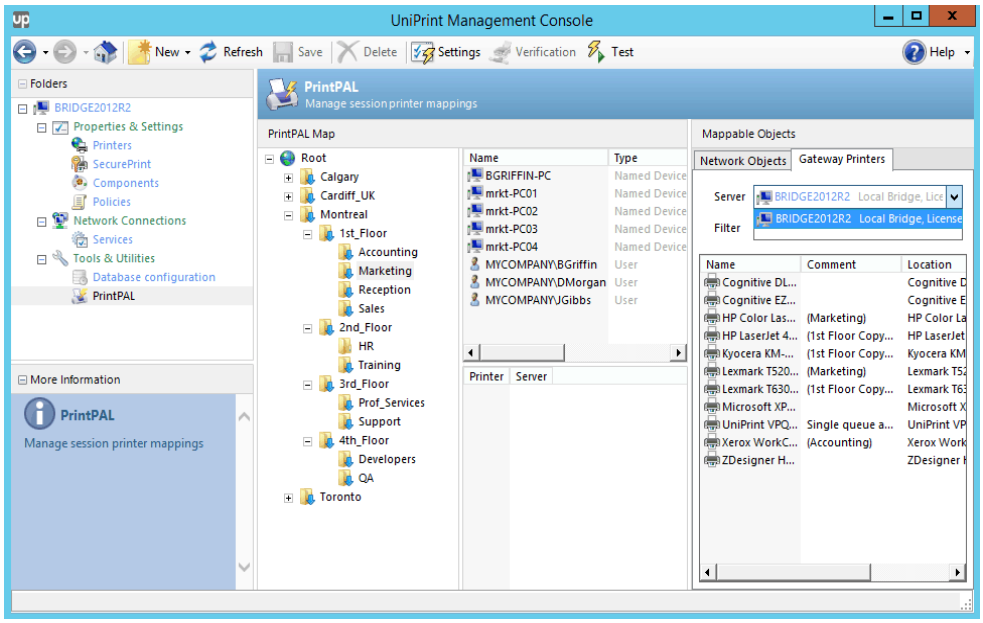


3. Under **PrintPAL Map**, click to select the group to which you want to map printers.

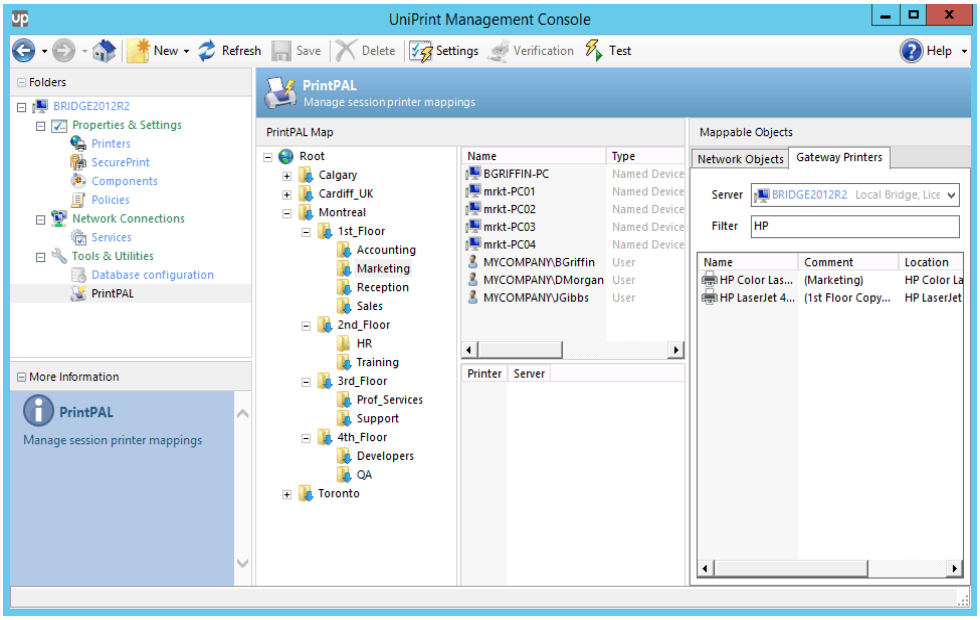
4. Under **Mappable Objects**, click the **Gateway Printers** tab.



5. From the **Server** list, select the UniPrint Bridge whose Gateway Printers you want to map.



a) Beside **Filter**, enter the character string with which to apply the filter to the resulting list and then press **ENTER**.

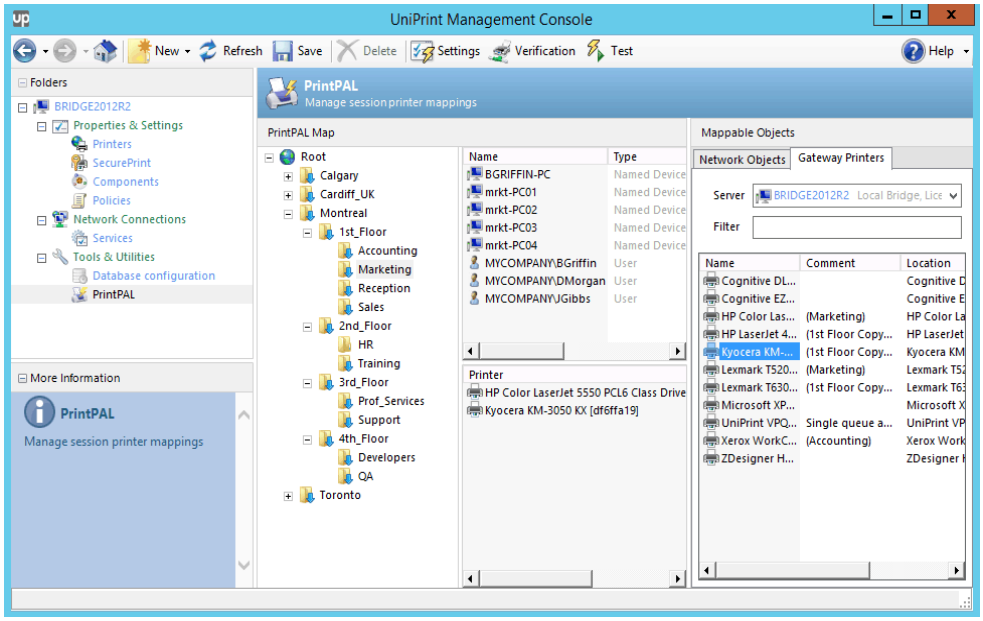


6. Click to select a Gateway printer and then either double-click it or press **ENTER** to add it to the PrintPAL map.

> **NOTE:** To add multiple printers that appear consecutively in the list, click the first printer you want to add, press **SHIFT** and then click the last printer. Press **ENTER** to add your selection to the PrintPAL map. To add multiple printers that do not appear consecutively in the list, click a printer, press **CTRL**, and then click the next printer. Press **ENTER** to add your selection to the PrintPAL map.

7. Repeat step 6, selecting groups and mapping printers as required.

8. Click **Save** to save your PrintPAL map.

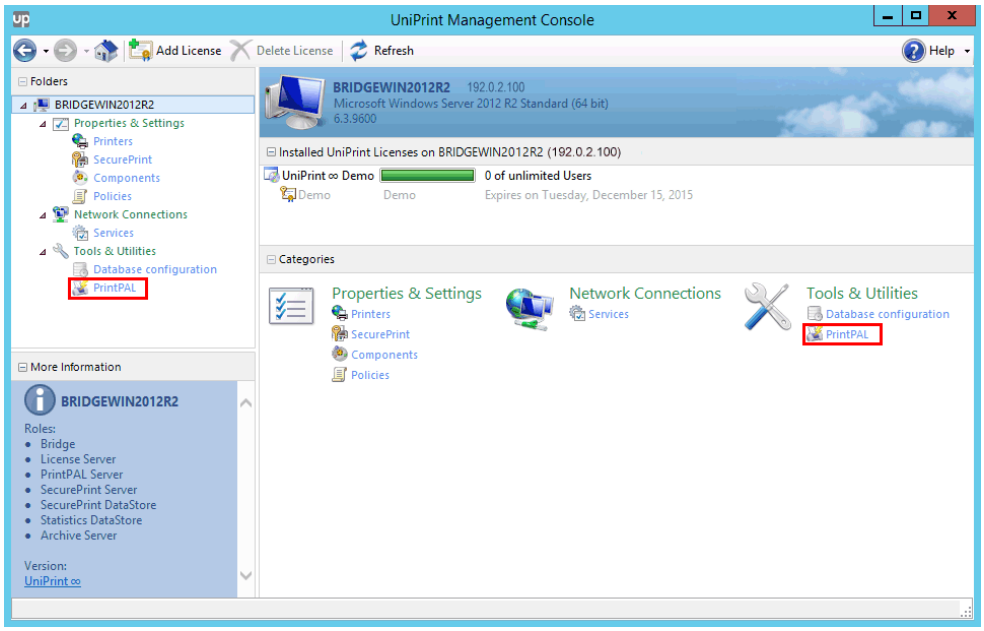


Setting Default Printers in PrintPAL

PrintPAL can be used to define the default printer for a group of devices. However, during an ICA/RDP session, a user can redefine their default printer through the Control Panel, if the administrator has enabled it.

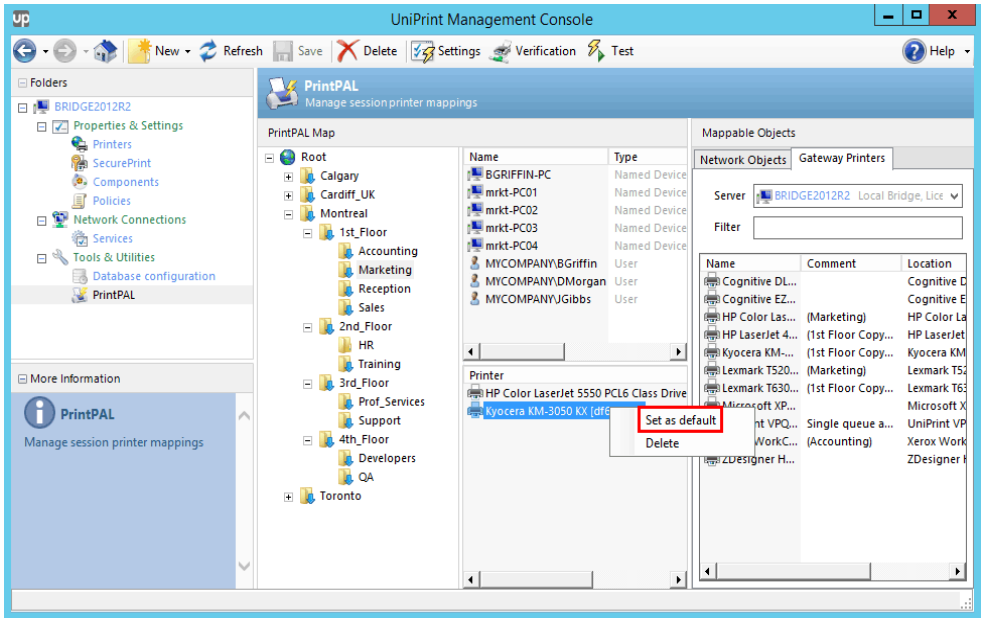
1. On the UniPrint Bridge, open the **UniPrint Management Console**.

2. Under **Tools & Utilities**, click **PrintPAL**.

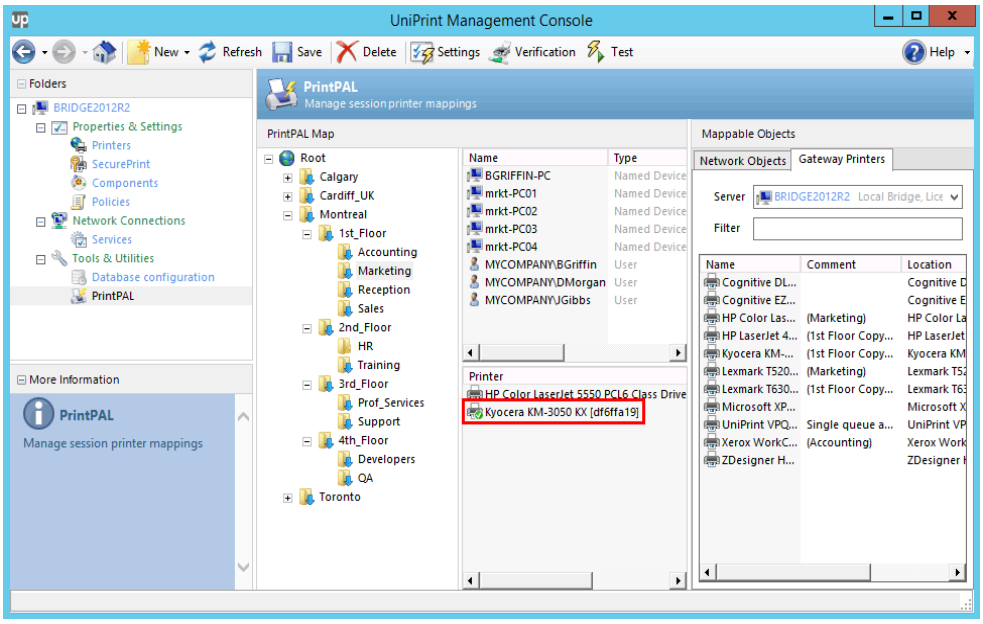


3. Under **PrintPAL Map**, click to select the group for which you want to define a default printer.

4. In the **Printers** list, right-click a printer and then select **Set as default**.



5. The default printer will be indicated with a green check mark. Click **Save** to save changes to the PrintPAL map.



NOTE: If multiple default printers are set, then PrintPAL will assign the default printer based on the following order of priority:

1. Device name
2. IP range
3. User name
4. Google account e-mail address

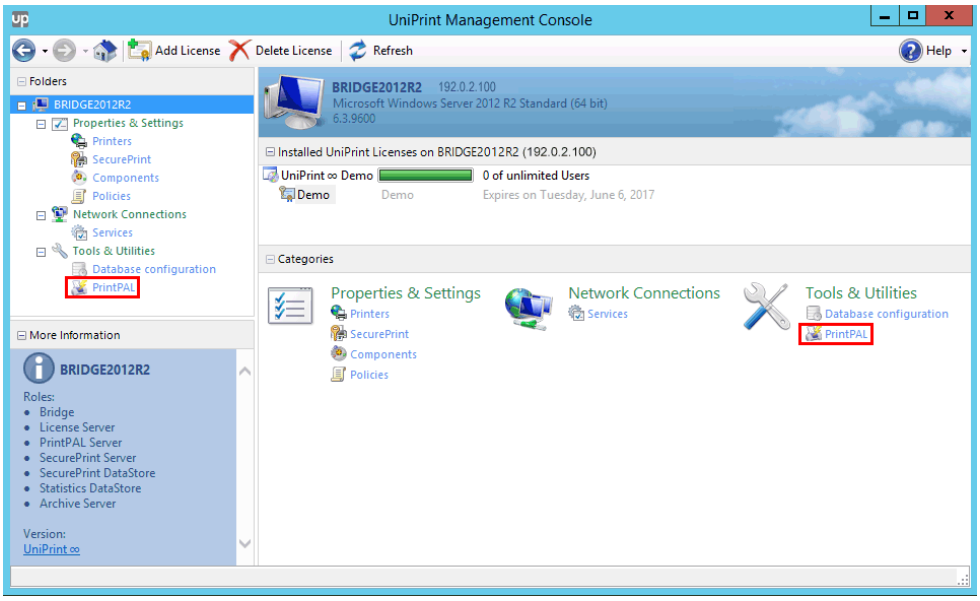
Enabling Local Gateway Queues in PrintPAL

Without requiring the Windows File and Printer Sharing ports to be open to the internet, users who log into an Application Server from an endpoint device that is not a member of the domain can still access and print to a Gateway printer by enabling local Gateway queues.

To enable a local Gateway queue for a specific printer, do the following:

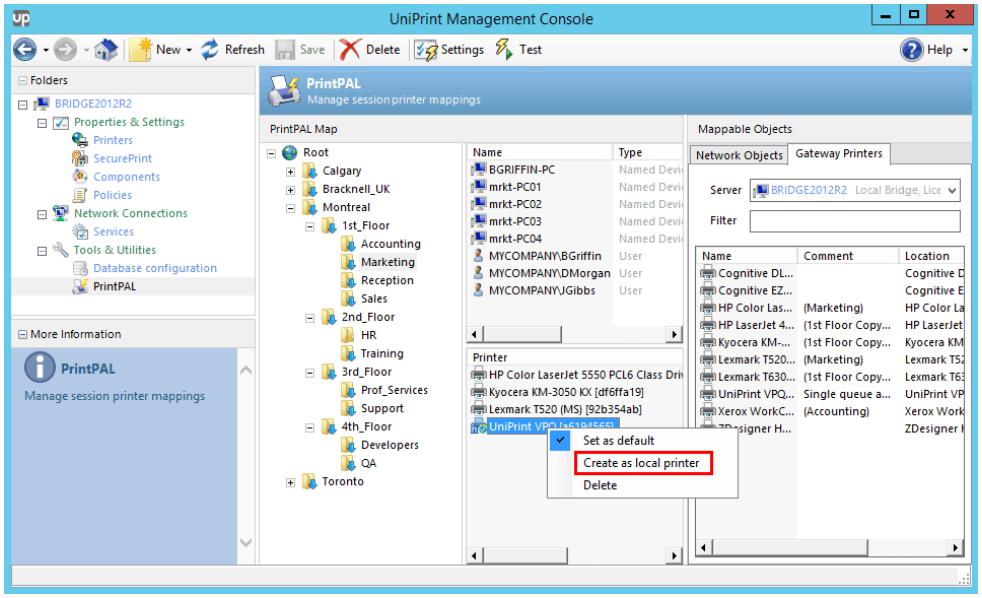
1. On the UniPrint Bridge, open the **UniPrint Management Console**.

2. Under **Tools & Utilities**, click **PrintPAL.**

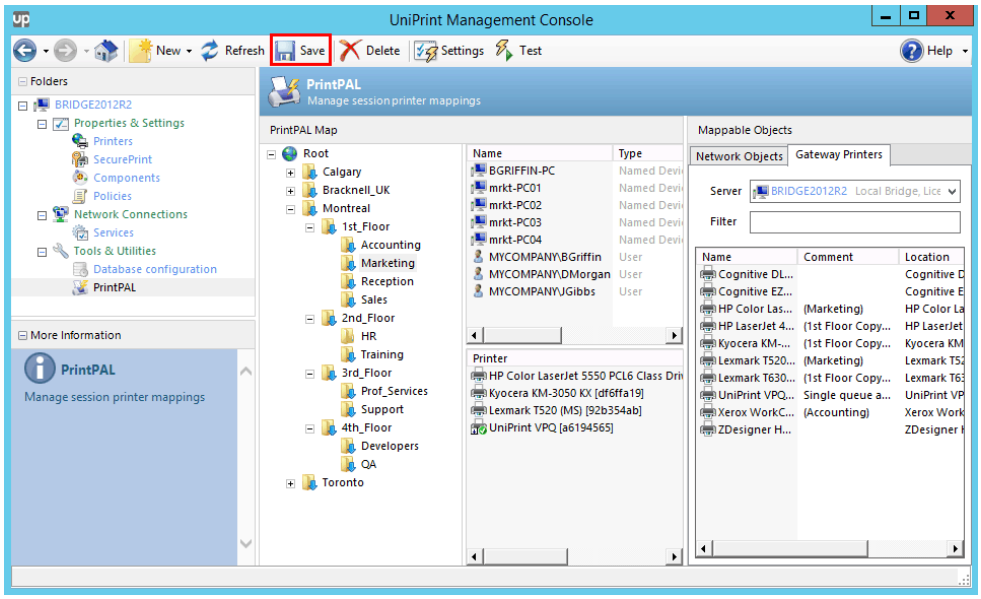


3. Under **PrintPAL Map**, click to select a group that has the desired printer mapped.

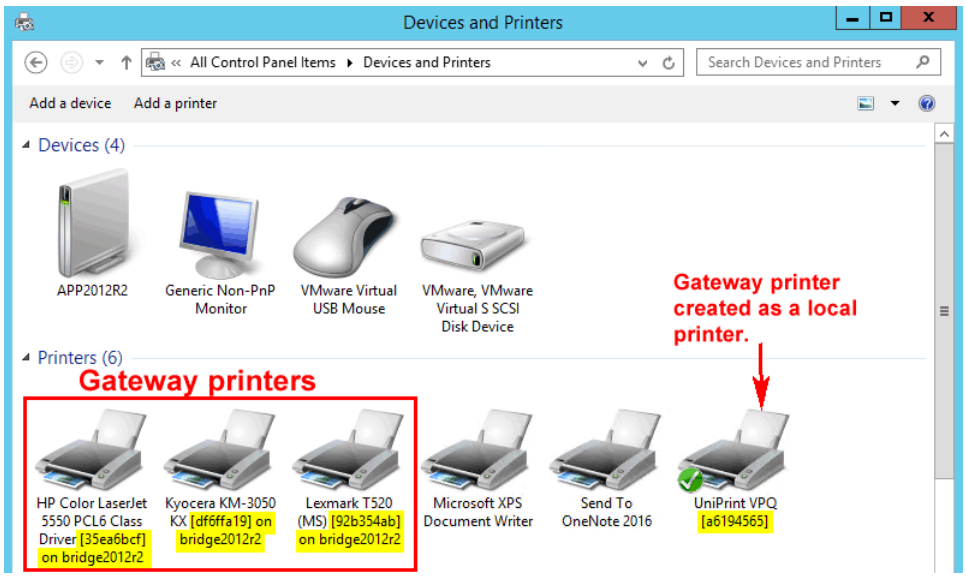
4. In the **Printers** list, right-click the printer and then select **Create as local printer**.



5. Click **Save**.



6. In the user's session, the hash number in square brackets indicates that the printer is a Gateway printer. However, the Gateway printer that has been created as a local queue, will not indicate from which server it is from.



NOTE: This local Gateway printer will be available to any user who logs into the application server and is not limited to the users within a specific PrintPAL group. Also deleting a locally created printer in the PrintPAL section of the UniPrint Management Console does not delete the printer from user sessions. To delete a locally created printer, the user is required to delete it through **Devices and Printers** within in their user session.

Testing Your PrintPAL Map

A testing utility has been provided to test your object-to-printer mapping. With complex mappings, the resulting printer list may not be obvious. You can test your PrintPAL map by device name, IP address, user name or you can test a current session.

How PrintPAL Determines Which Printers to Map

This testing utility mimics PrintPAL and searches the map in the following order to decide which printers to map to a session:

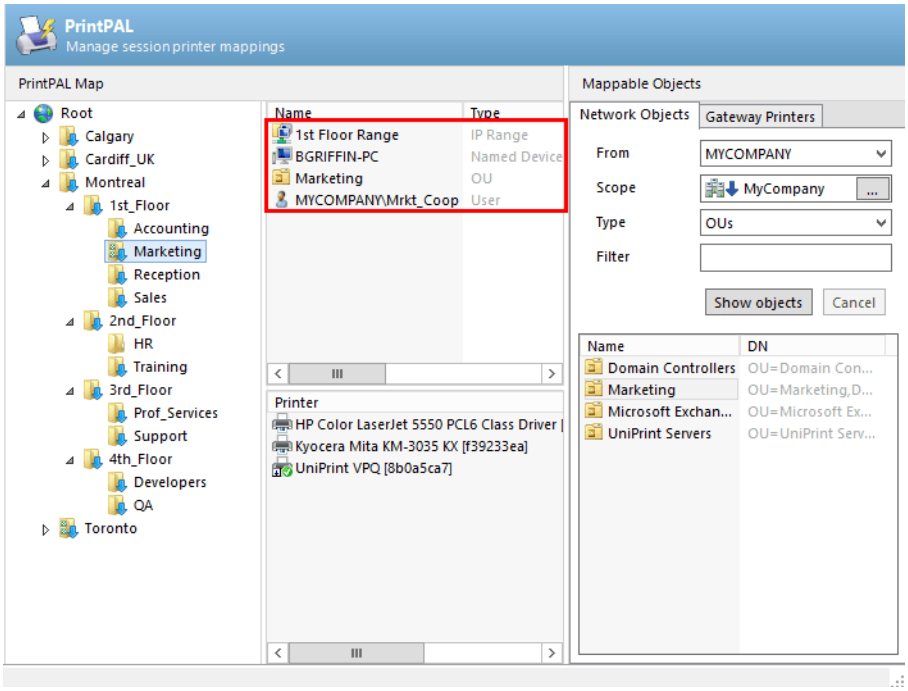
1. Device name or wildcard
2. Device OU
3. Device IP address or IP address range (IPv4)
4. User name
5. User group
6. User OU

EXAMPLE: In a PrintPAL map a named device has been mapped to Printer A and an IP range is mapped to Printer B. If this named device has an IP address within the IP range, the test utility and PrintPAL will map Printer A to the session and will not continue to map any printers mapped to subsequent parameters. The result of using this utility is a consolidated list of which printers are mapped to a particular session.

Enabling the **Match all criteria types** option changes how PrintPAL decides which printers to map to a session. In order for printers to be mapped the following statement must be TRUE: (*DeviceName* **OR** *OU*) **AND** *DeviceIPAddress* **AND** (*UserName* **OR** *UserGroup*).

EXAMPLE: The **Marketing** group is created with **Inherit printers from parent group** and **Match all criteria types** enabled.

A named device, an IP range, an OU, and a user are mapped to the Marketing group. The OU contains a group of devices and a user group.



The three printers will only be mapped to a session that is logging on from BGRIFFIN-PC or from a device listed in the OU ***and*** from within the 1st Floor IP range ***and*** logged in as Mrkt-Coop or is listed in the OU.

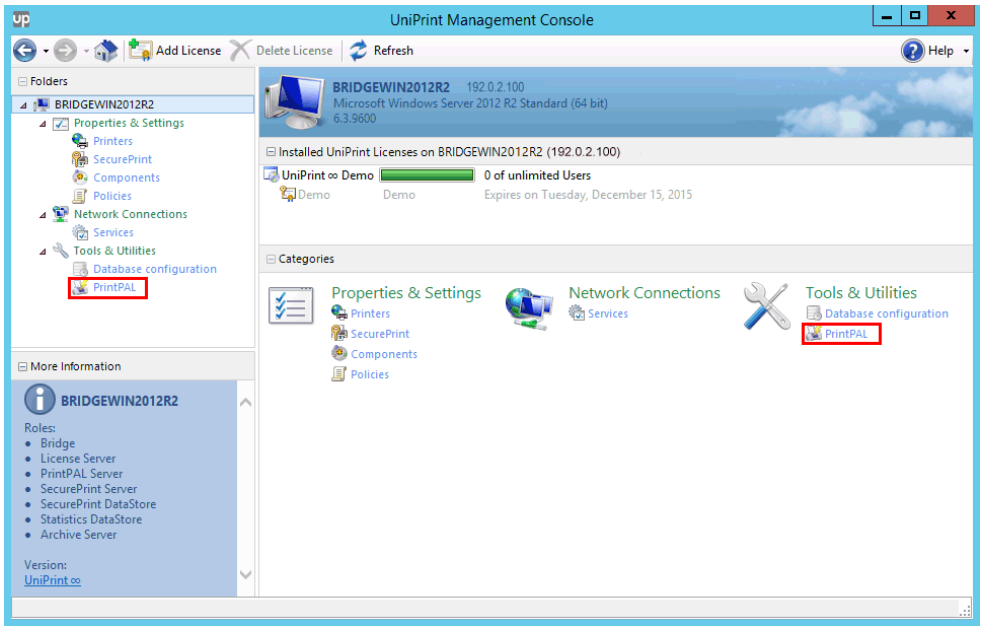
If the **Match All** option is not selected then printers will be mapped to a session as long as ***any one*** of the conditions are met. Therefore, any user or

device within the Marketing OU, any user logging in from BGRIFFIN-PC, any device logging in with an IP address within the 1st Floor IP Range or Mrkt-Coop logged in from any device and from any IP will have these printers mapped to their session.

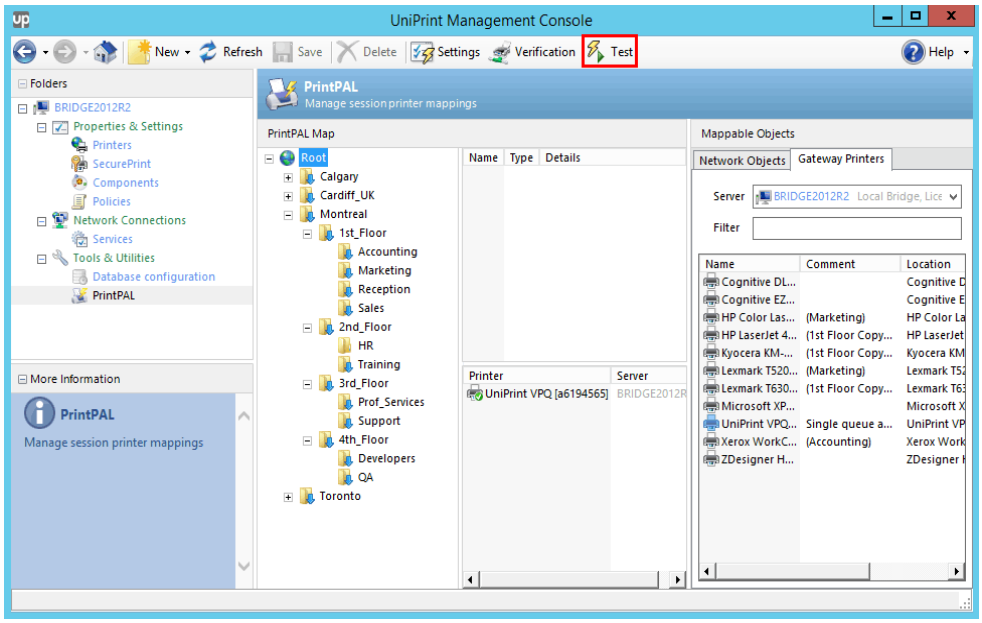
Testing By Device Name, IP Address or User Name

1. On the UniPrint Bridge, open the **UniPrint Management Console**.

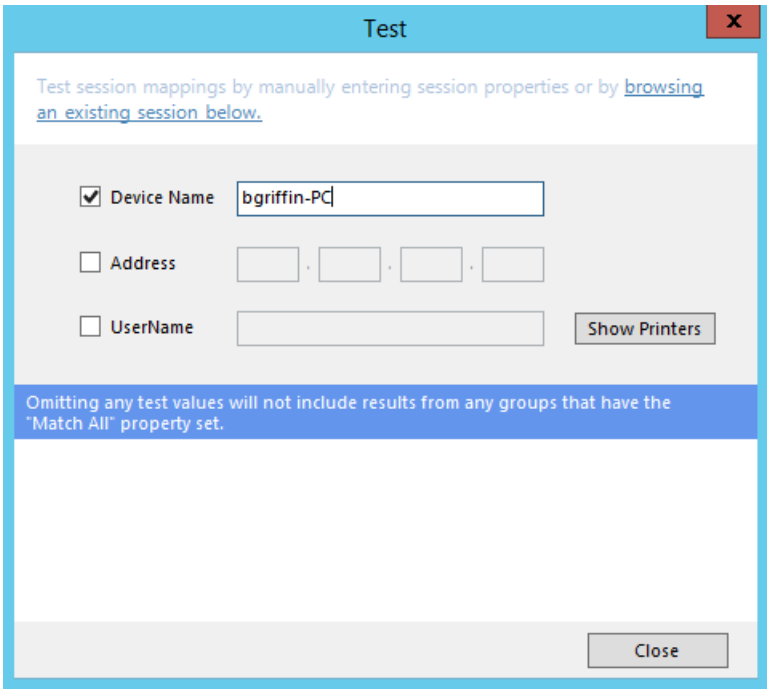
2. Under **Tools & Utilities**, click **PrintPAL**.



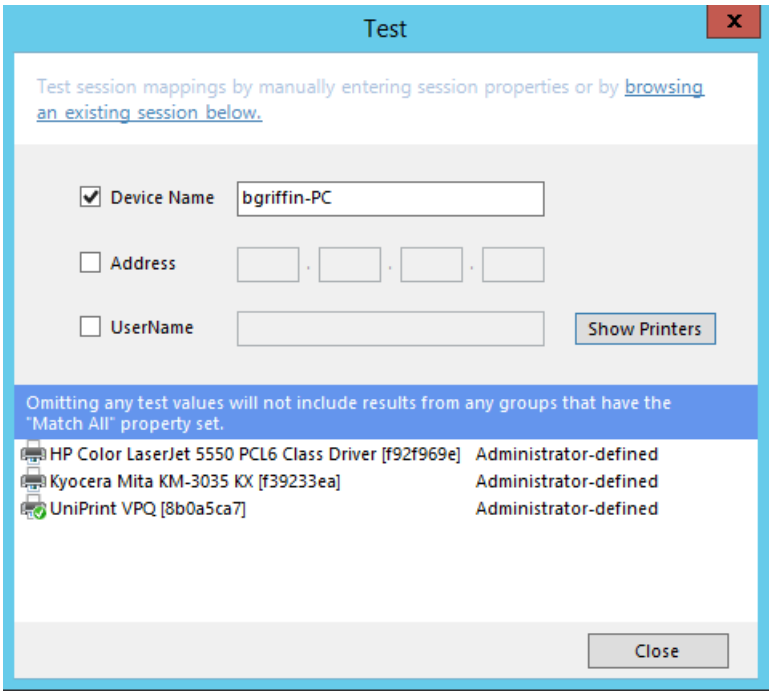
3. Click **Test**.



4. Select the object you would like to test. For example, device name, IP address or user name and then enter the parameter to test. Click **Show Printers**.



5. All of the Gateway printers that are mapped to that particular object should appear in the printer list.

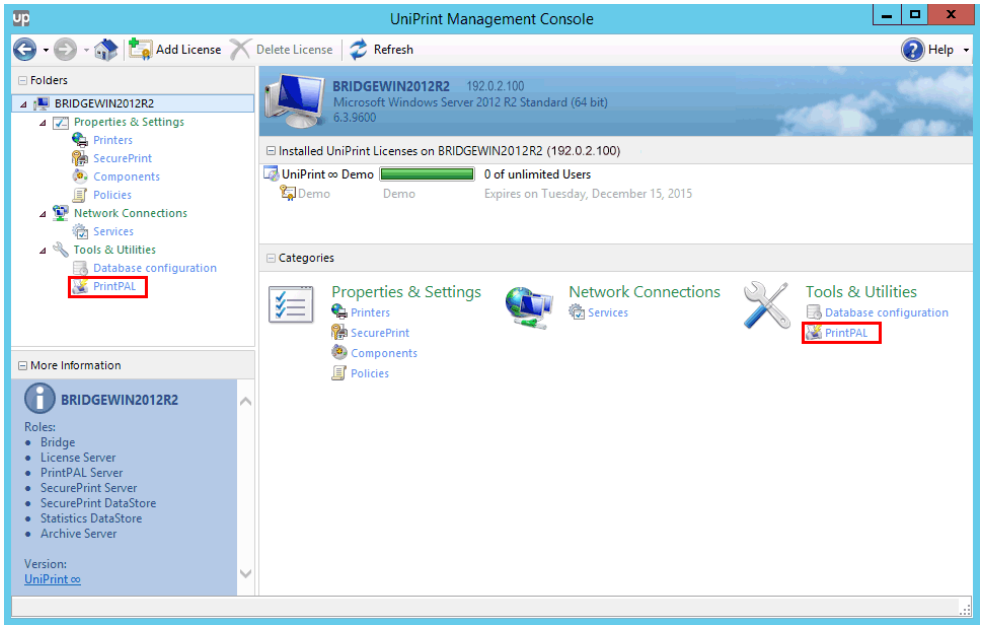


6. Click **Close** to exit testing.

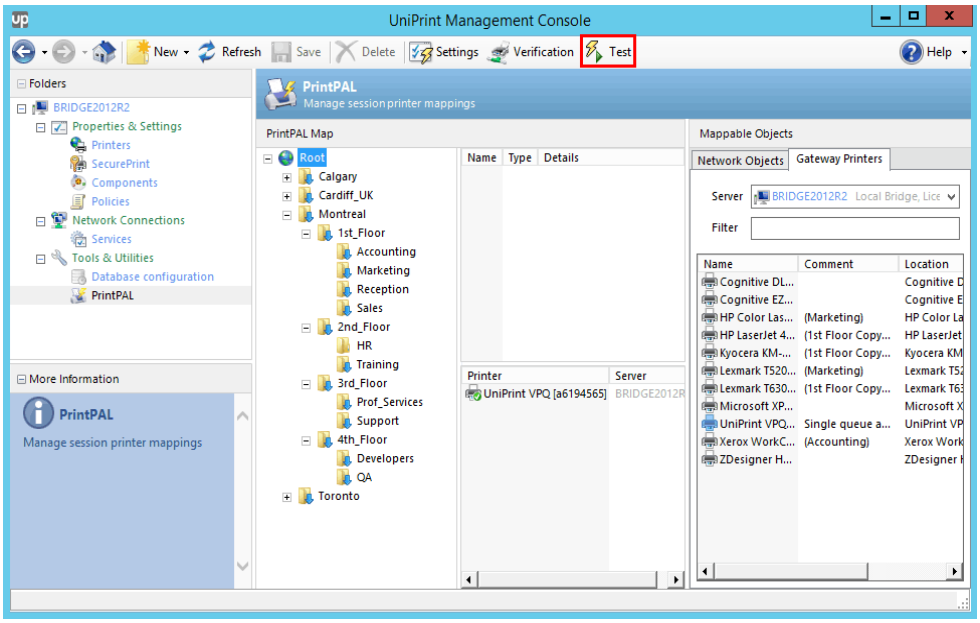
Testing A Current Session

1. On the UniPrint Bridge, open the **UniPrint Management Console**.

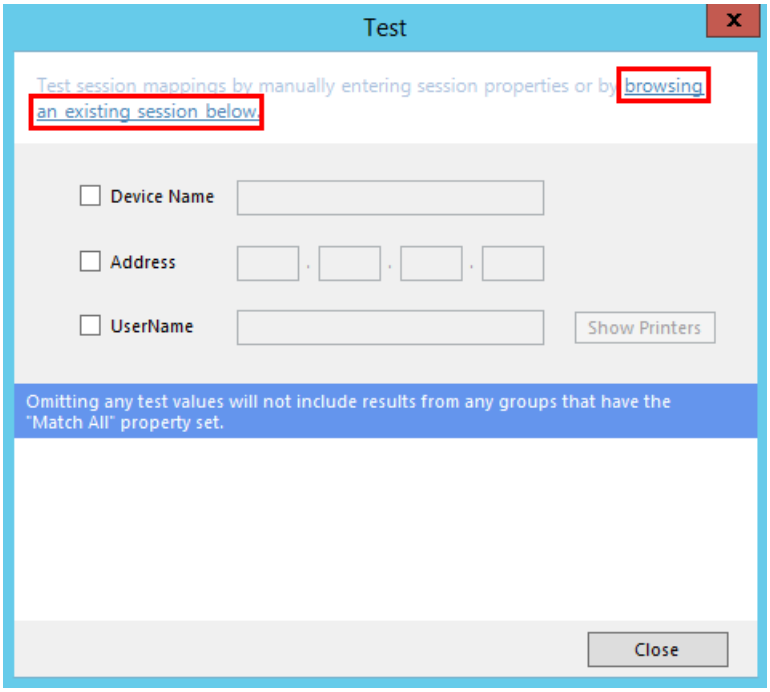
2. Under **Tools & Utilities**, click **PrintPAL**.



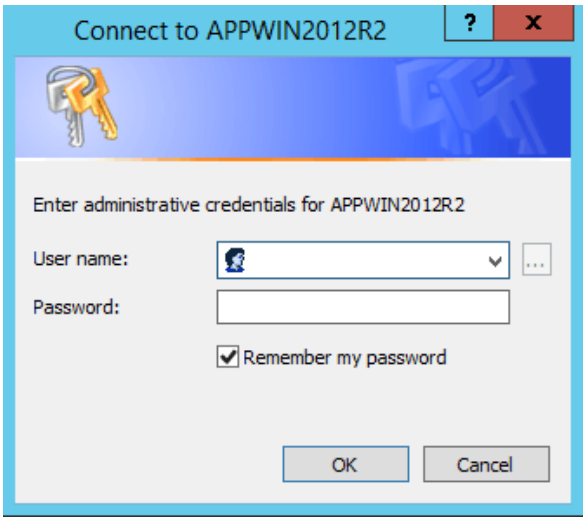
3. Click **Test**.



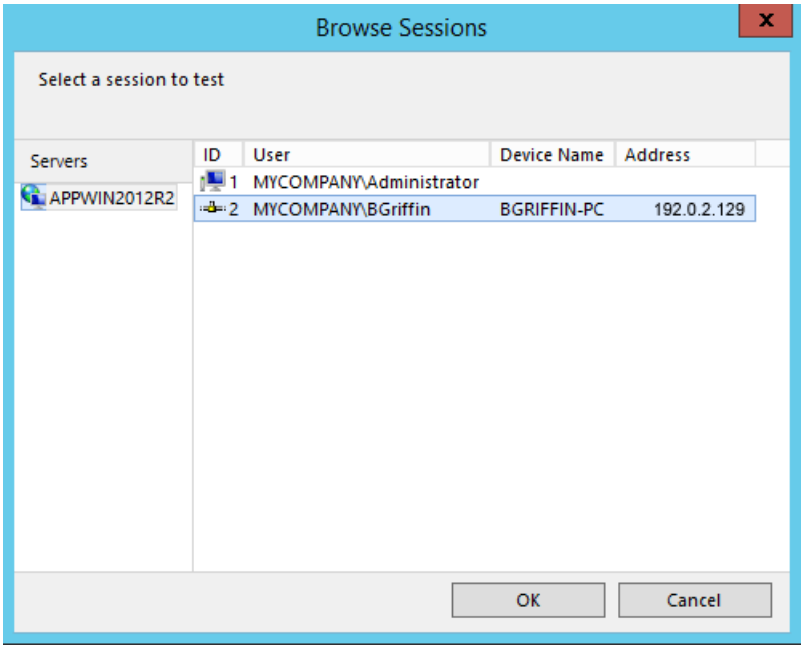
4. Click **browsing an existing session below**.



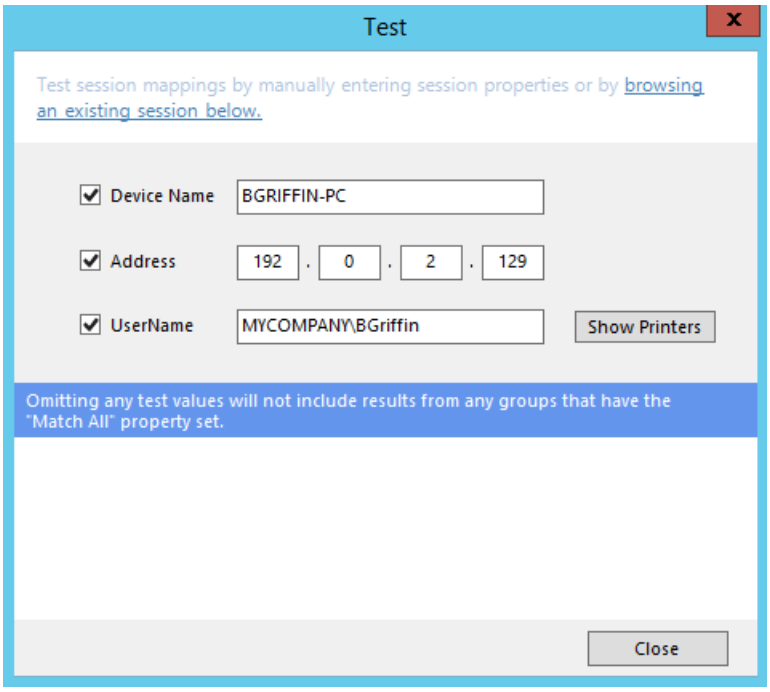
5. Enter your administrative credentials for the Application Server and then click **OK**.



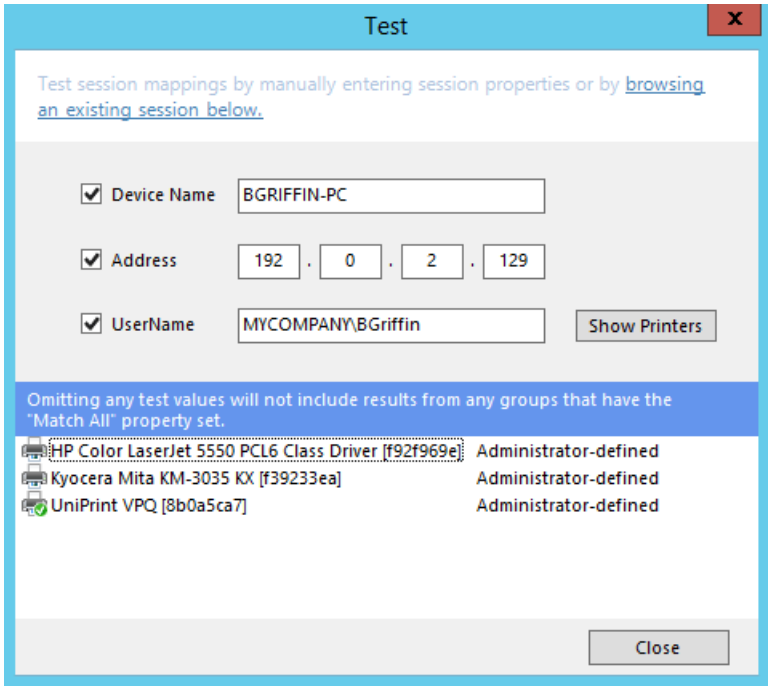
6. Click to select the session to test and then click **OK**.



7. The **Device Name**, IP **Address** and **UserName** parameters will be populated. Click **Show Printers**.



8. All of the Gateway printers that are mapped to this session will appear in the printer list. Click **Close** to exit testing.

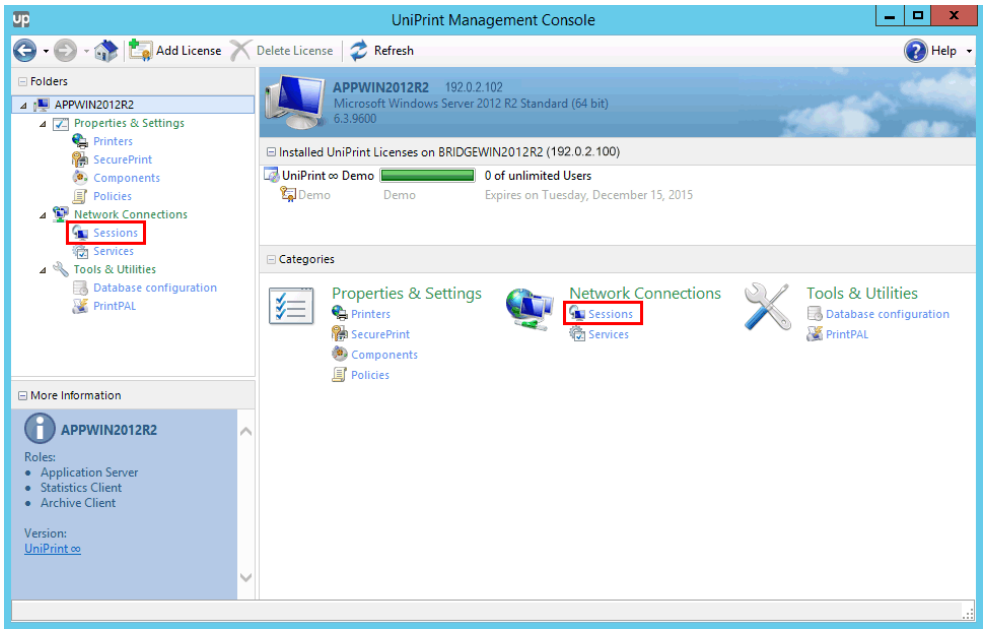


Setting PrintPAL To Automatically Map Printers When A Session Is Started

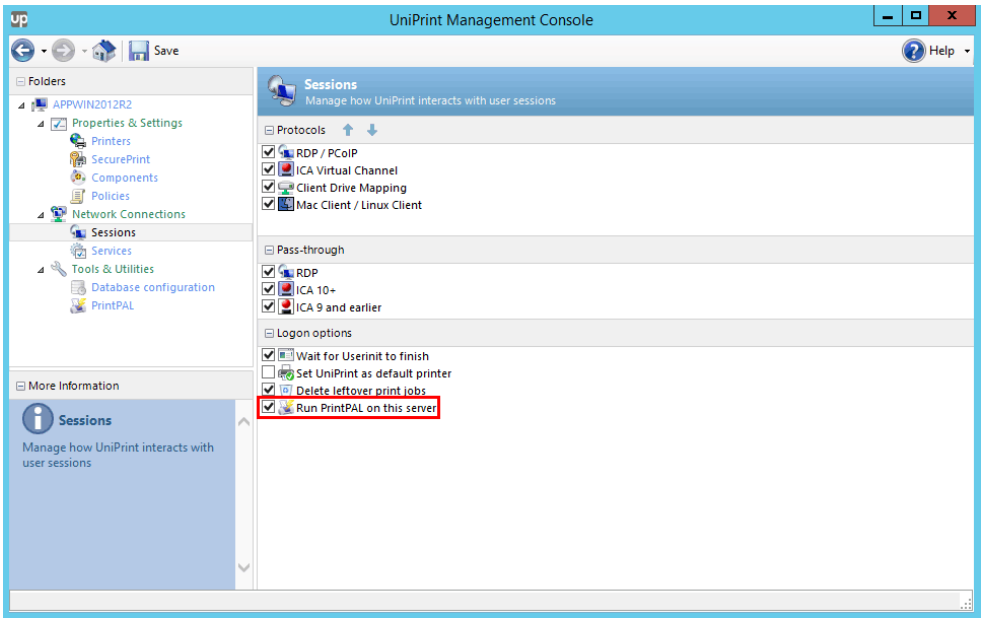
PrintPAL can be set to automatically run and map printers to the user's session when the user launches a session on the UniPrint Application Server.

1. On the UniPrint Application Server, open the **UniPrint Management Console**.

2. Under **Network Connections**, click **Sessions**.



3. Under **Logon options**, select **Run PrintPAL on this server** and then click **Save**.



Setting PrintPAL To Delete and Then Remap Printers in a Session

By default, if a printer connection already exists in a session, PrintPAL will not attempt to remap the printer. However, at times, it may be necessary to delete a printer mapping and then remap it to a session if certain configuration settings are altered.

WARNING! Instructing PrintPAL to delete and then remap printers will result in user settings being deleted. Use this registry key with caution if users want their printer settings to remain persistent from session to session.

To automatically have PrintPAL delete and then remap printers, do the following:

1. On the UniPrint Application Server, click **Start** and then type `Run`. Double-click **Run**.

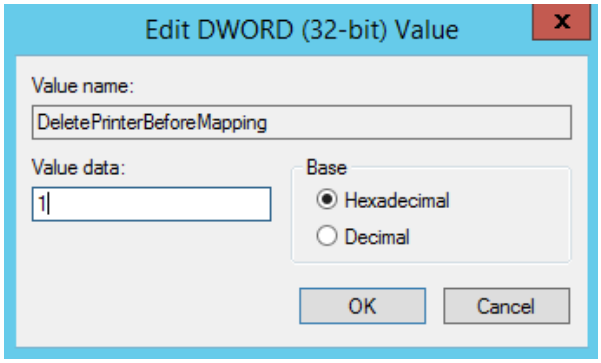
2. Type `regedit` to edit the registry.

3. In the registry editor, expand the **HKEY_LOCAL_MACHINE\SOFTWARE\UniPrint\Session** key.

4. In the **Edit** menu, click **New** and then select **DWORD (32-bit) value**.

5. Name this new value **DeletePrinterBeforeMapping** and then double-click **DeletePrinterBeforeMapping**.

6. If a printer connection already exists in a session and to force PrintPAL to delete the printer and then remap it, set **DeletePrinterBeforeMapping** to `1`. Click **OK**.



7. Close the Registry Editor.

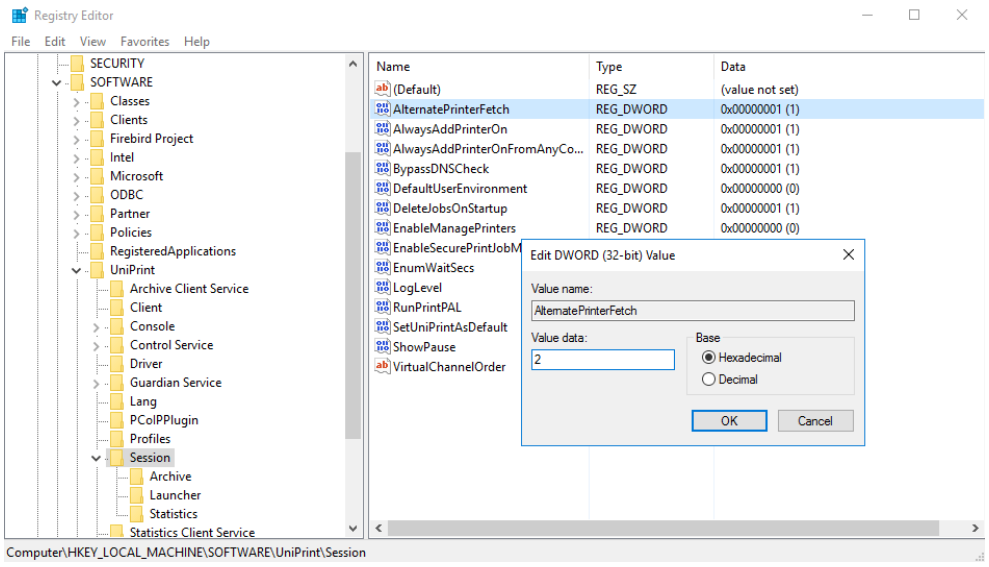
Setting PrintPAL Communication to Use JSON

If PrintPAL is set to use JSON, printer information retrieval is faster and reduces network traffic. This alternative method is recommended for large printer deployments.

To set PrintPAL to use JSON, do the following:

1. On the Application Server, open the registry editor.

2. Under **HKEY_LOCAL_MACHINE\Software\UniPrint\Session**, set **AlternatePrinterFetch** to **2**.



3. Close the Registry Editor.

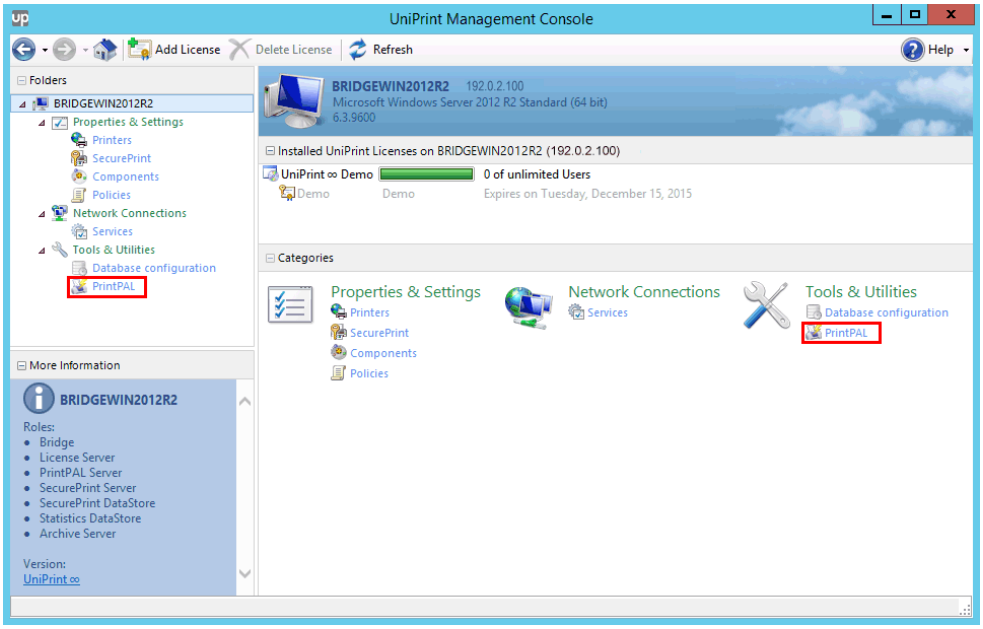
Discovering Orphaned Printers and Printers With Offline Status

For large environments with hundreds of printers, keeping track of printers that have been deleted from the Print Server, but not off the Bridge and printers that have an inoperative status can be daunting. Typically, when a printer is decommissioned, administrators know to automatically remove the driver from the Print Server, but they tend to forget that an enumerated instance also exists on the Bridge. This creates orphaned printers and could result in mapping issues in PrintPAL.

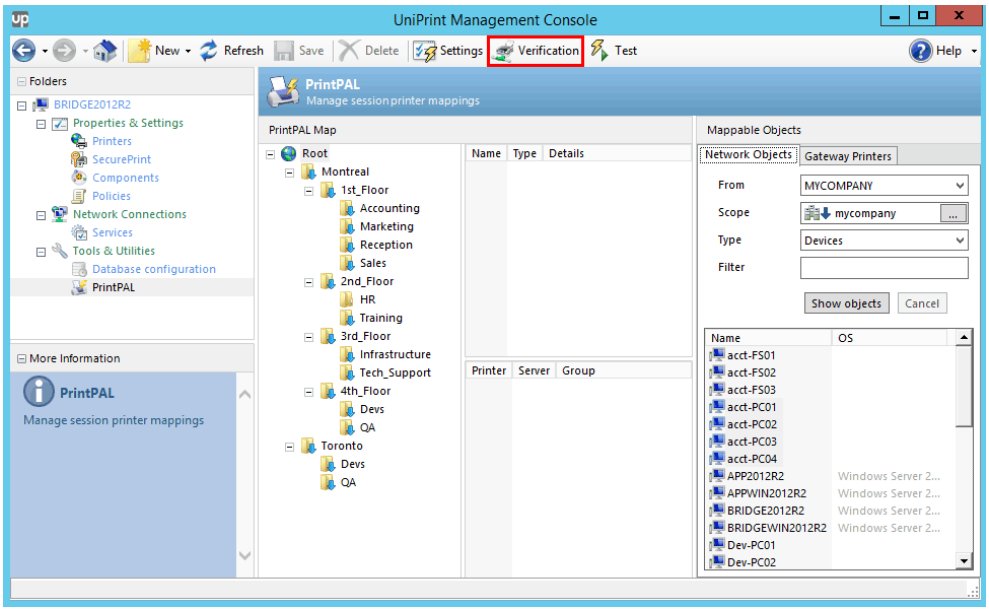
To generate of list of orphaned and inoperative printers use the Verification tool in PrintPAL.

1. On the UniPrint Bridge, open the **UniPrint Management Console**.

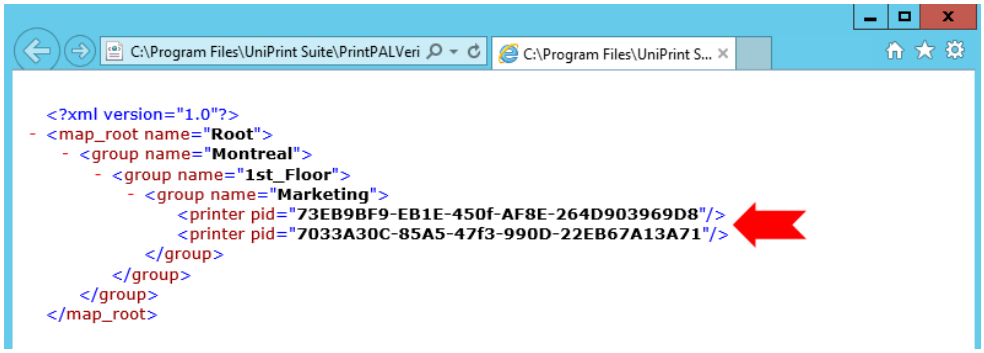
2. Under **Tools & Utilities**, click **PrintPAL**.



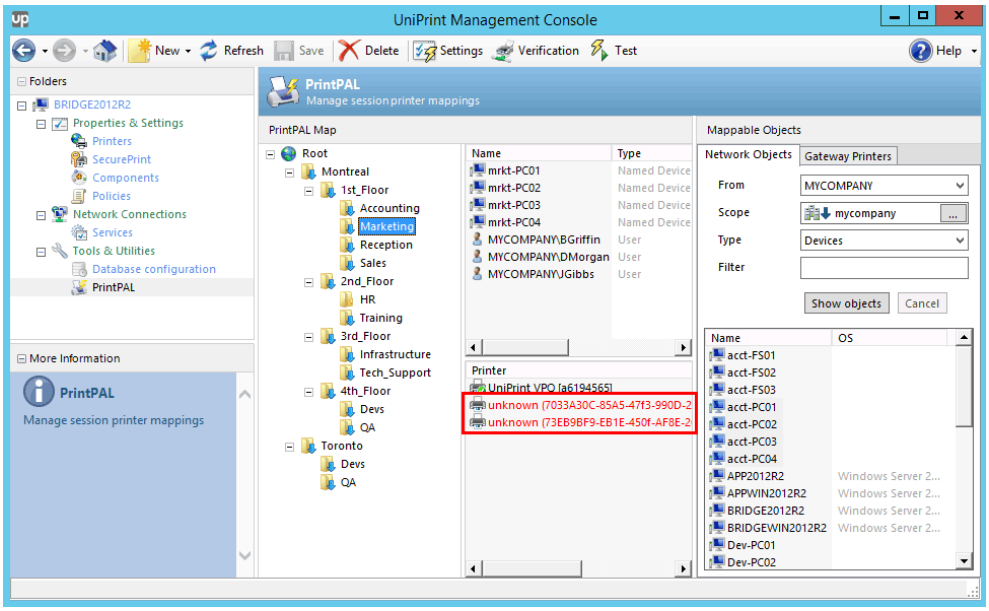
3. Click **Verification** and an XML report will appear with a list of orphaned and inoperative printers.



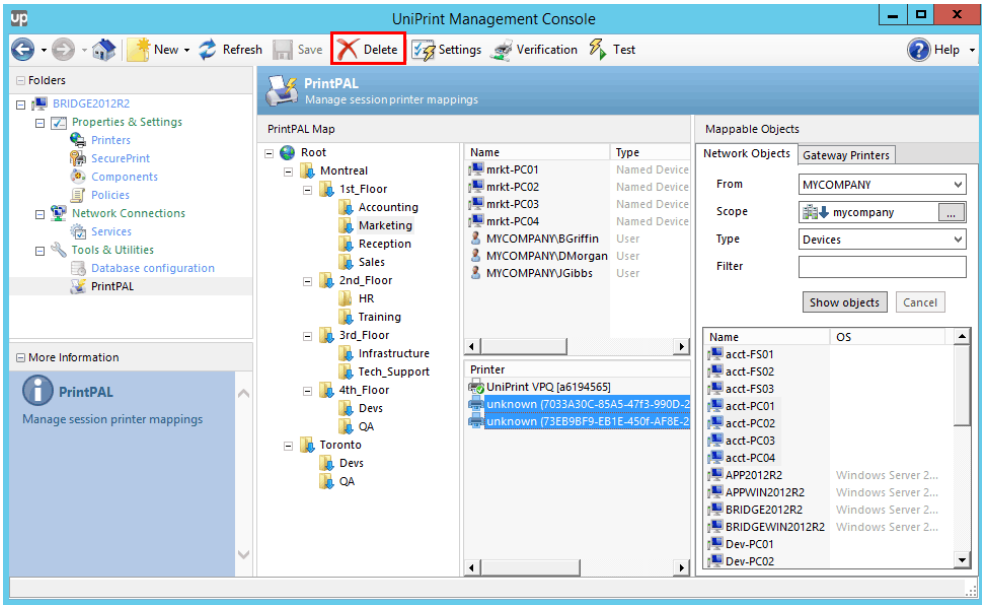
4. The XML report displays the path for the inoperative printers. The example XML report below displays two inoperable printers mapped to the Marketing department on the 1st Floor in Montreal.



5. In PrintPAl, by following the path in the XML report, the map will display the inoperable printer in red.



6. The administrator can then go the printer to fix the issue or if the printer has been decommissioned, the printer can be deleted from the PrintPAL and a replacement printer can be mapped to the group.



CHAPTER 8

UniPrint Infinity

Configuring SecurePrint

The complete SecurePrint solution incorporates the vPad or vPad CE, the SecurePrint Server, Datastore and Virtual Print Queue (VPQ). These components work together to provide efficient and secure pull-printing, while helping to increase corporate sustainability.

In addition to pull print printing, SecurePrint can also be used for print stream compression. Print Stream Compression was initially designed for environments where the print server is located in a central data center and a set of printers are located remotely in a different geographical location. Print Stream Compression will compress the print data transmitted from the central print server to the vPad or vPad CE device by utilizing the UniPrint Transport Port Monitor. Print Stream Compression is recommended for print server consolidation initiatives.

Configuring UniPrint SecurePrint

WARNING! In order to utilize encryption, all domain-level certificates must be up-to-date and valid on all UniPrint Bridges. For more information, see http://support.microsoft.com/kb/929103.

Installing the UniPrint vPad Device

Before installing the vPad ensure that you have the power cable (included) and a network cable.

1. Find an appropriate location to mount the vPad device.

2. Insert the power cable into the bottom of the vPad device.

3. Insert the network cable into the bottom, left-most connector of the vPad device.

4. Connect the network cable into a network outlet, switch or router.

5. Plug the device into an electrical outlet.

6. Power on the vPad and it will automatically detect the closest UniPrint Print Server.

Installing the vPad CE Device

Before installing the vPad CE, ensure that you have the micro USB power supply (included) and a network cable. Unlike the vPad, the vPad CE does not require user interaction and can be installed anywhere in your remote location.

1. Insert the power cable into the micro USB port located on the side of the vPad CE device.

2. Insert the network cable into the end of the vPad CE device.

3. Connect the network cable into a network outlet, switch or router.

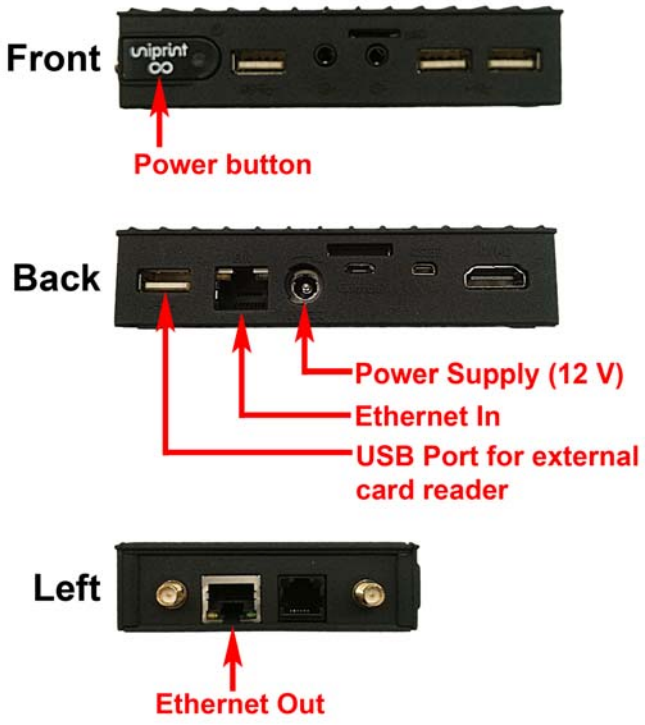
4. Plug the power supply into an electrical outlet.

NOTE: Unlike the vPad device, the vPad CE does not have a power switch. To reboot the vPad CE, simply unplug the electrical supply and plug it back in.

Once connected to the network, the vPad CE will be assigned an IP address through DHCP. The vPad CE will then attempt to connect to a UniPrint Print Server that has SecurePrint print server components installed. If the vPad CE is unable to connect to a Print Server or it connects to the wrong Print Server, additional configuration is required, see "Configuring the vPad CE to Connect to the UniPrint Print Server" on page 208 for detailed configuration steps.

Installing the vPad CE2 Device

Before installing the vPad CE2, ensure that you have the 12V power supply (included) and a network cable. Similar to the vPad CE, the vPad CE2 does not require user interaction and can be installed anywhere in your remote location. The advantage of the vPad CE2 over the vPad CE, is mostly enhanced operation. Its functions and features are similar to the vPad CE since it supports Print Stream Compression and with an external RFID/HID reader it can be used to "tap & release" print jobs. This latest addition to the vPad family is faster and has more ports available, including a second built-in Ethernet port.



1. Insert the power supply into the back of the device.

2. Insert the network cable into the Ethernet port at the back of the device.

   a) Optionally, plug in an external card reader into a USB port. ***Note**: Depending on your network setup, you may also want to connect another network cable for outbound traffic and use the vPad CE2 as a switch. To do this, connect a second network cable to the Ethernet port on the left side of the vPad CE2.*

3. Connect the first network cable into a network outlet, switch or router.

4. Plug the power supply into an electrical outlet.

5. Push the power button on the front to turn on the device and the vPad CE2 will automatically be assigned an IP through DHCP.

Running the SecurePrint Emulator

For testing purposes, the SecurePrint emulator has been provided. By running the emulator on a workstation, you can mimic how the actual vPad device will work in your environment. This workstation must be connected to the network in order for the emulator to automatically discover your print servers.

To launch the SecurePrint emulator, do the following:

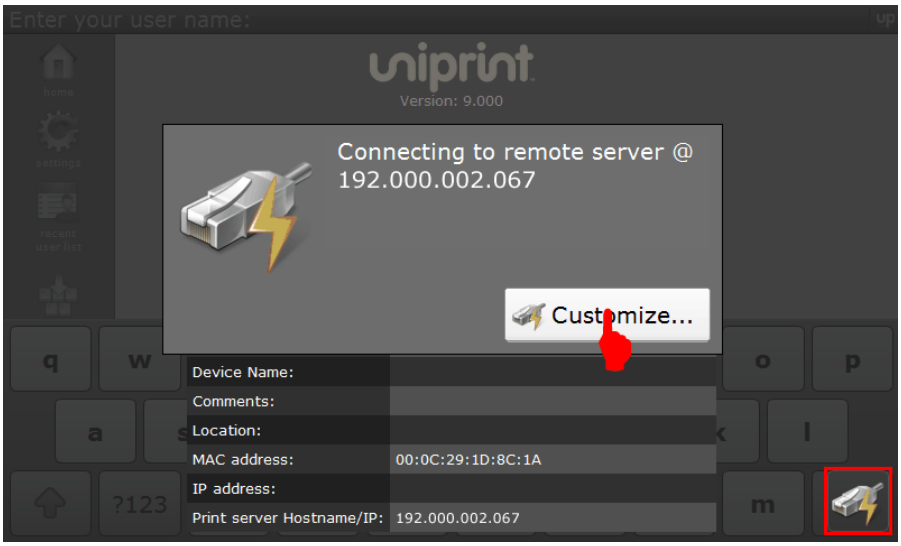
- From the UniPrint Infinity installation package, run the self-extracting executable file, **SecurePrint Emulator.exe**.

Activating the UniPrint vPad

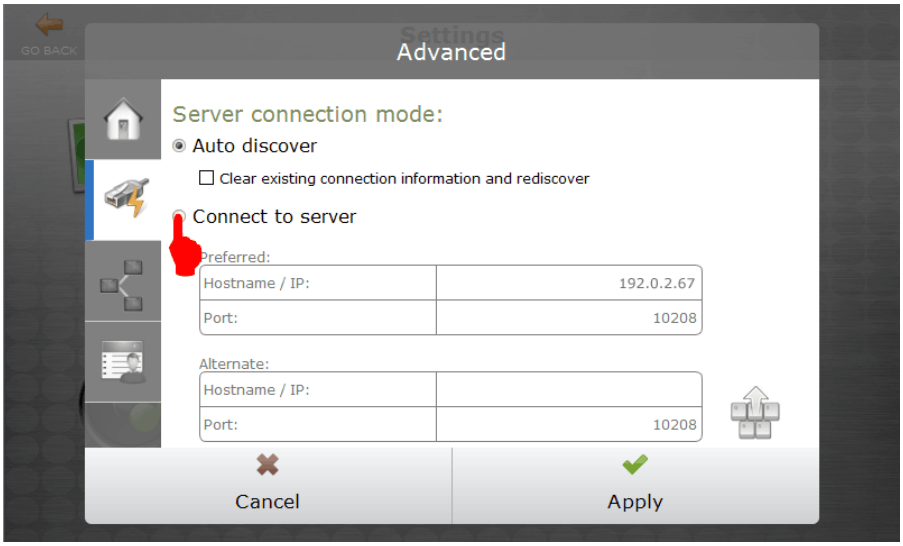
Follow these instructions for both the vPad device and the SecurePrint emulator.

1. Ensure that the vPad is connected to the correct UniPrint Print Server that has **SecurePrint print server components** installed. If the

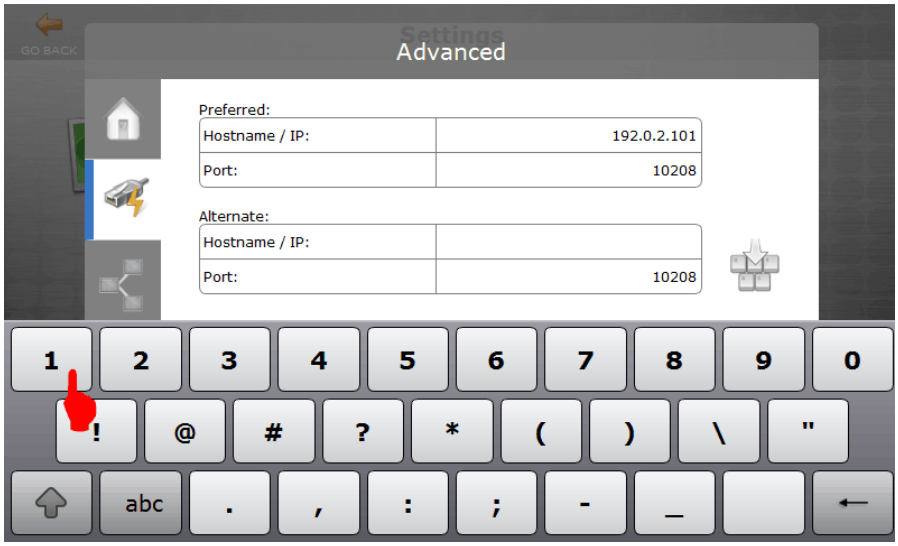
Print Server Hostname or IP address is pointing to the wrong UniPrint Print Server, tap **Customize**.



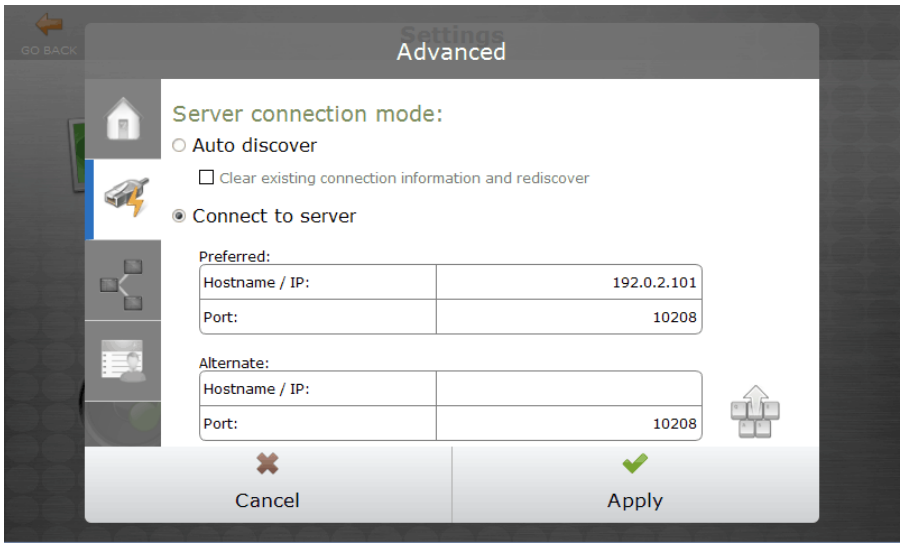
a. Tap **Connect to server**.



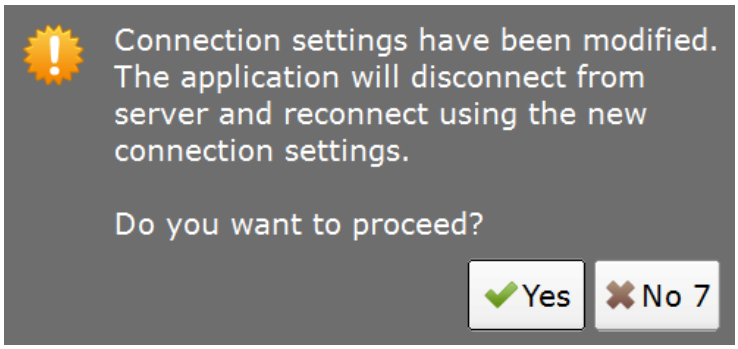
b. Change the IP address or hostname to that of the desired UniPrint Print Server and then tap to minimize the keypad.



c. Tap **Apply**.

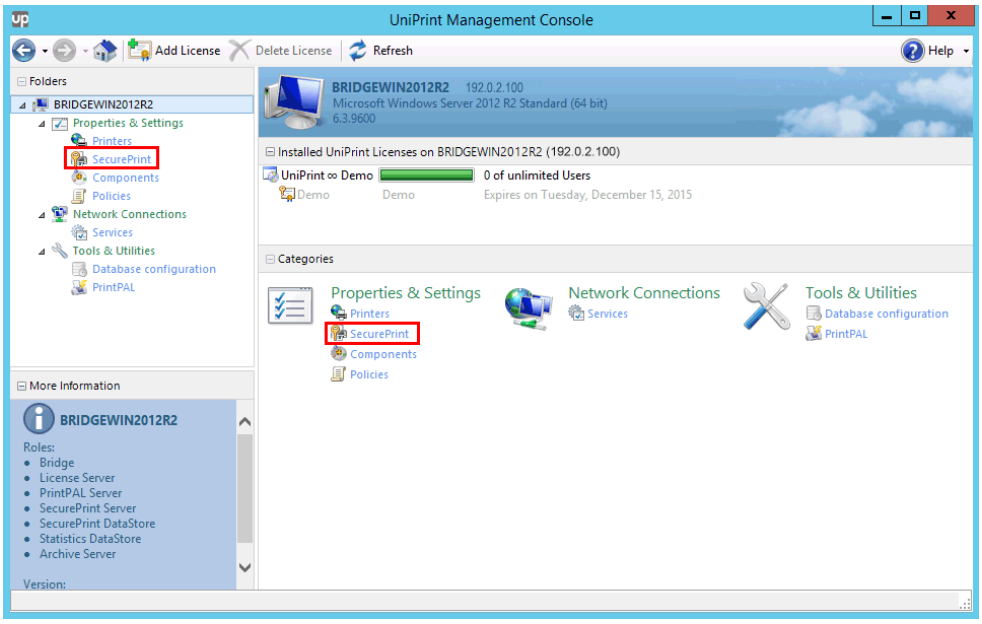


d. Tap **Yes**.



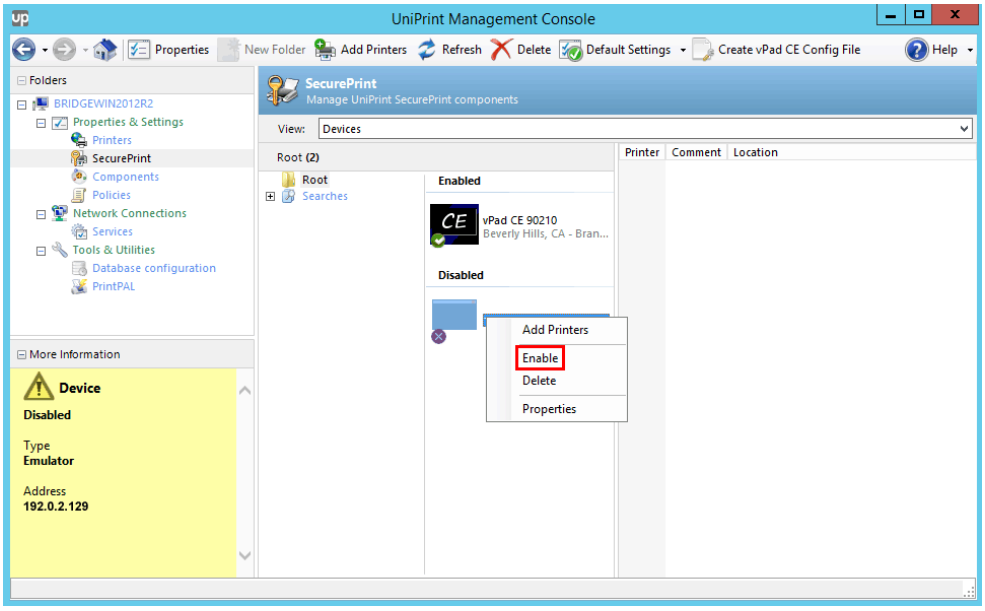
2. From a UniPrint component, open the **UniPrint Management Console**.

3. Under **Properties & Settings**, click **SecurePrint**.

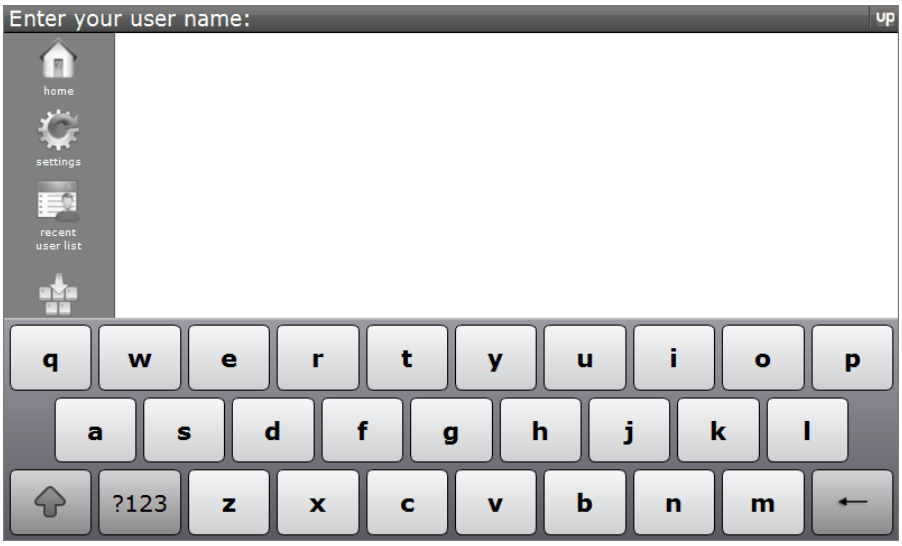


4. Click **Refresh** if the vPad does not immediately appear.

5. Right-click the vPad device and then select **Enable**.



6. Once enabled, return to the vPad and the user name entry screen should appear.



Configuring the vPad CE to Connect to the UniPrint Print Server

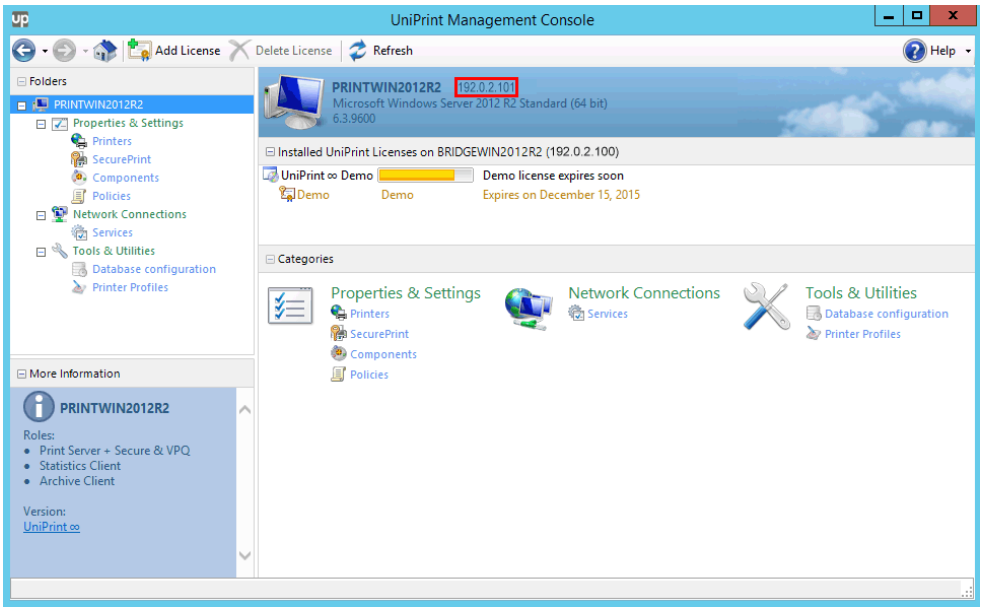
Since the vPad CE device lacks a display screen, the procedure to "activate" the vPad CE differs from that of the vPad device or SecurePrint Emulator.

There are two ways to configure the vPad CE. The first method requires an empty USB flash drive and the second method accesses the vPad CE through a web interface.

Using SecurePrint.ini on a USB Flash Drive

This method requires an empty USB flash drive. The capacity of the flash drive does not need to be large – a 512 MB flash drive will suffice.

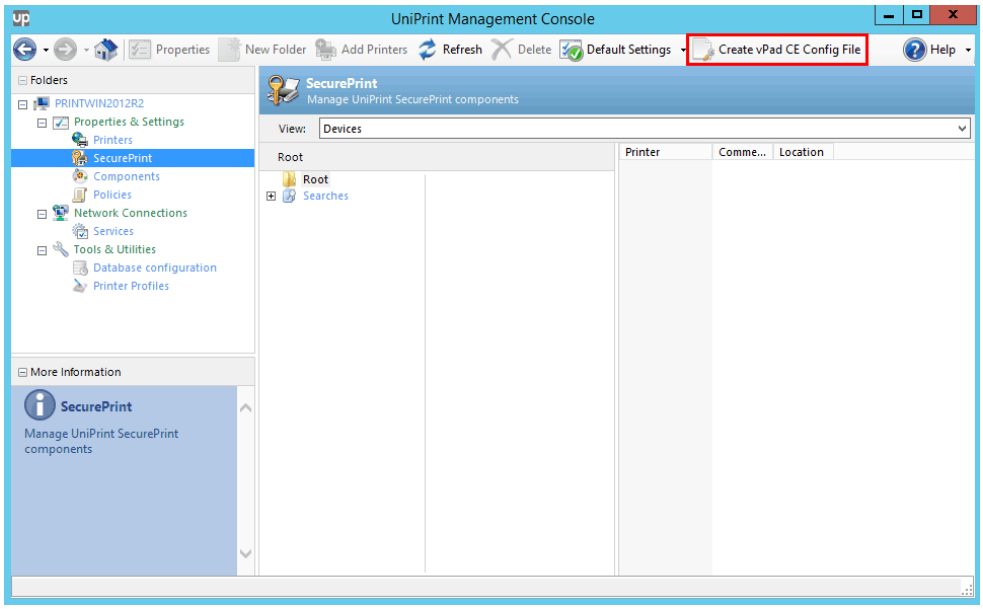
1. On the **Print Server**, open the **UniPrint Management Console** and take note of the IP address.



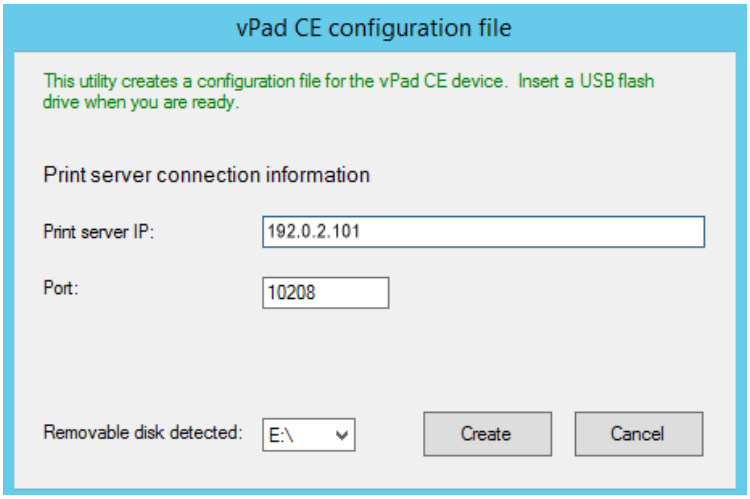
2. Under **Properties & Settings**, click **SecurePrint**.

3. Click **Refresh** to ensure that the vPad CE has not been discovered. If it has been discovered, this procedure is unnecessary.

4. If the vPad CE fails to appear in the vPad list, click **Create vPad CE Config File**.



5. Enter the **Print Server IP** address and **Port** number (if necessary). Insert an empty flash drive into a USB port on the Print Server and then click **Create**.



6. A file called **SecurePrint.ini** will be created in the root directory of the flash drive. Click **OK** to clear the confirmation message.

7. Eject the flash drive from the print server.

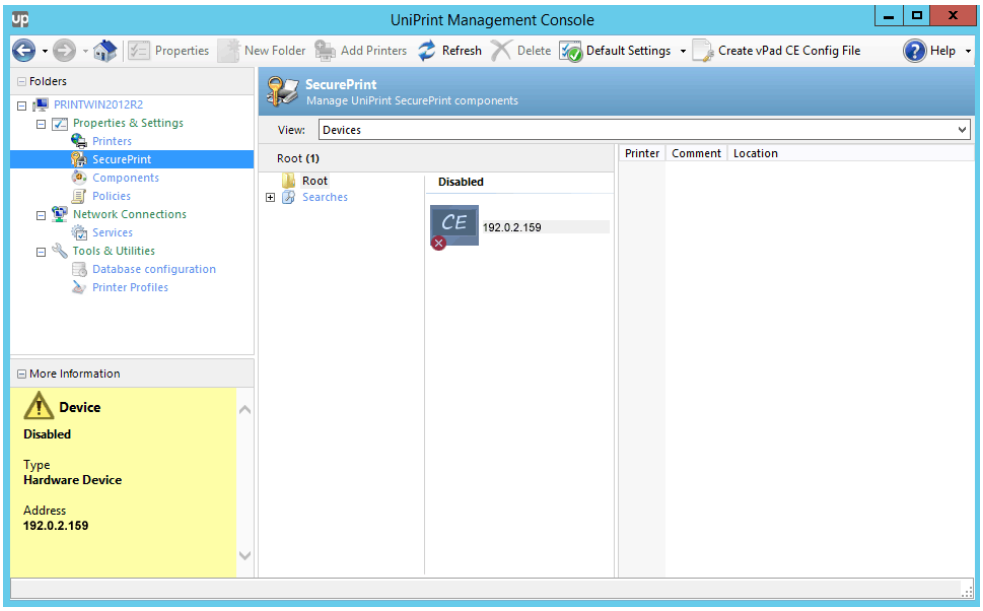
8. SecurePrint.ini can also be edited at this point using Notepad.

   a) Open SecurePrint.ini in Notepad and any of the following:

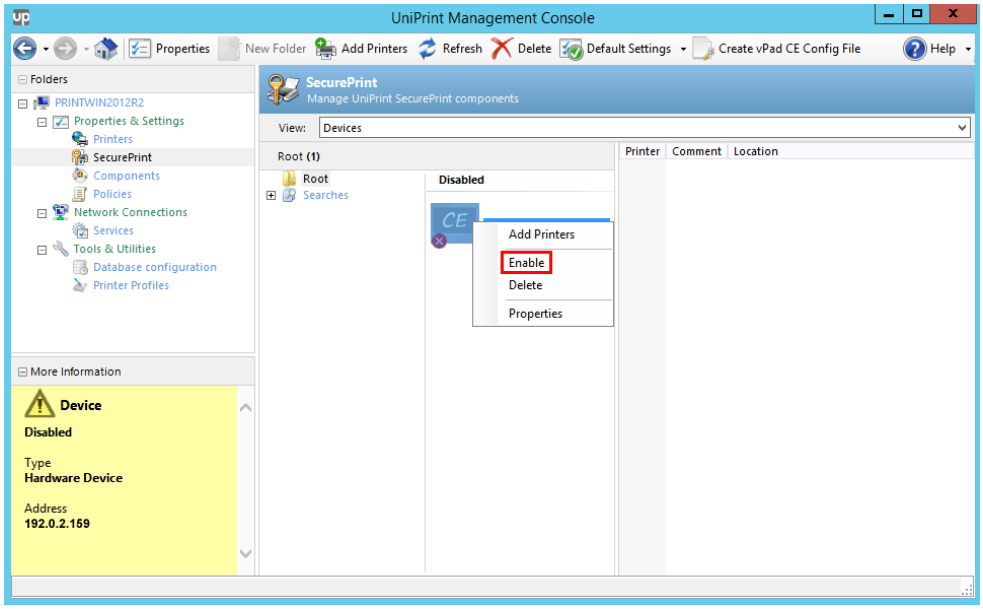
9. Insert USB flash drive into the vPad CE.

10. Unplug the power cable from the vPad CE and then plug it back in again to reboot the device.

11. Click **Refresh** and the vPad CE should appear in the vPad list.

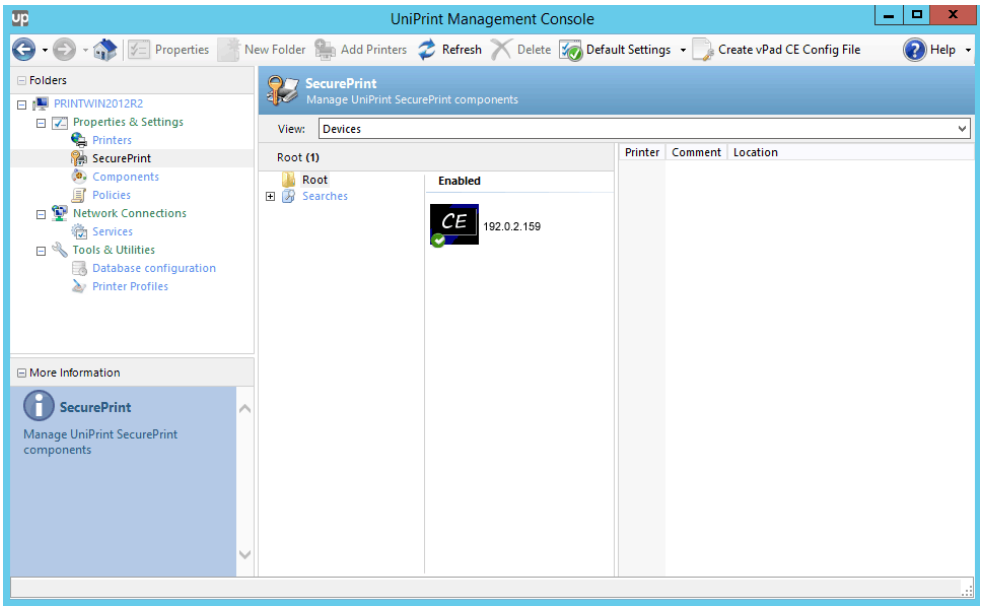


12. Right-click the vPad CE and then select **Enable**.



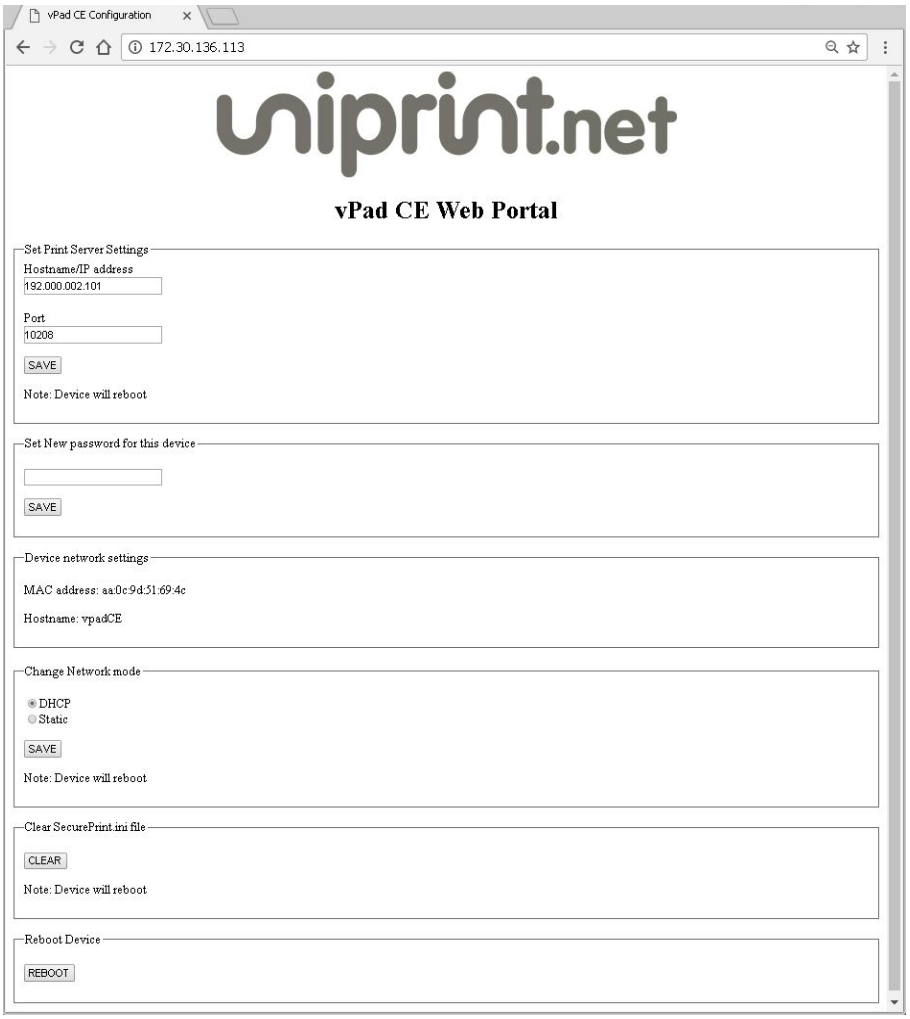
13. Proceed by changing the properties of the vPad CE and then enable print stream compression, see "Enabling Data Compression Between Print Server And Printer Through The vPad" on page 261 or to use the vPad CE with an internal or external card reader, assign a printer and import a list of user names and card IDs. See "Adding Printers to

the vPad" on page 233 and "Importing A List Of Users and Smart Card IDs Into SecurePrint" on page 242.



Using the vPad CE Web Interface

If the IP address of the vPad CE is known, administrators can access various configuration settings for the vPad CE directly through its web interface. To access the web interface, in a web browser, enter the IP address of the vPad CE.



Change any of the following settings as required.

Setting	Description
Set Print Server Settings	Enter the IP address or hostname and port number of the UniPrint Print Server to which the vPad will connect. Click **Save** and the vPad CE will restart automatically.
Set New password for this website	Enter a new password for this web interface and then click **Save**. ***Note****: The user name is* ***UniPrint****.*
Device network settings	Displays the MAC address of the vPad CE.
Change Network Mode	Sets how this vPad CE will be assigned an IP address. Click **Save** and the vPad CE will restart automatically.

Setting	Description
Clear SecurePrint.ini file	To set the settings back to the original default settings, click **Clear**. The vPad CE will restart automatically.
Reboot Device	To restart the vPad CE, click **Reboot**.

Troubleshooting: vPad Pro/CE Cannot Connect to the UniPrint Print Server

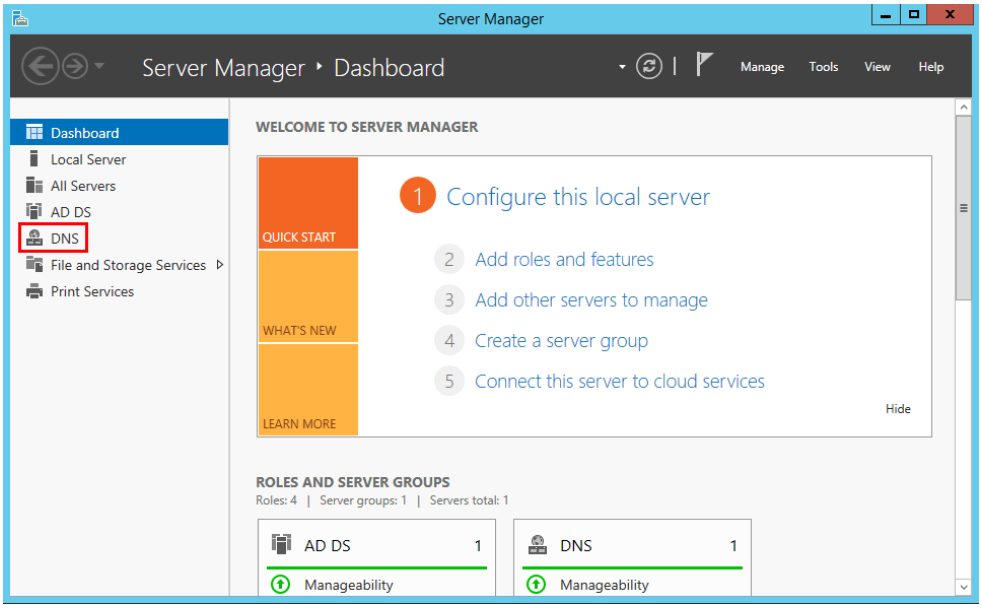
In the situation whereby the vPad Pro/CE is being installed by a non-technical person at a remote location, they may experience issues trying to connect to the UniPrint Print Server. The typical methods for connecting to the UniPrint Print Server as outlined in previous sections requires knowledge of the IP address or host name of the UniPrint Print Server, which this person may not have, or USB access to the UniPrint Print Server, which maybe locked down for security reasons.

The recommended method to circumvent this issue is to create an Alias, **UPPrintServer**, for the UniPrint Print Server on your DNS server and then restart the vPad Pro/CE device.

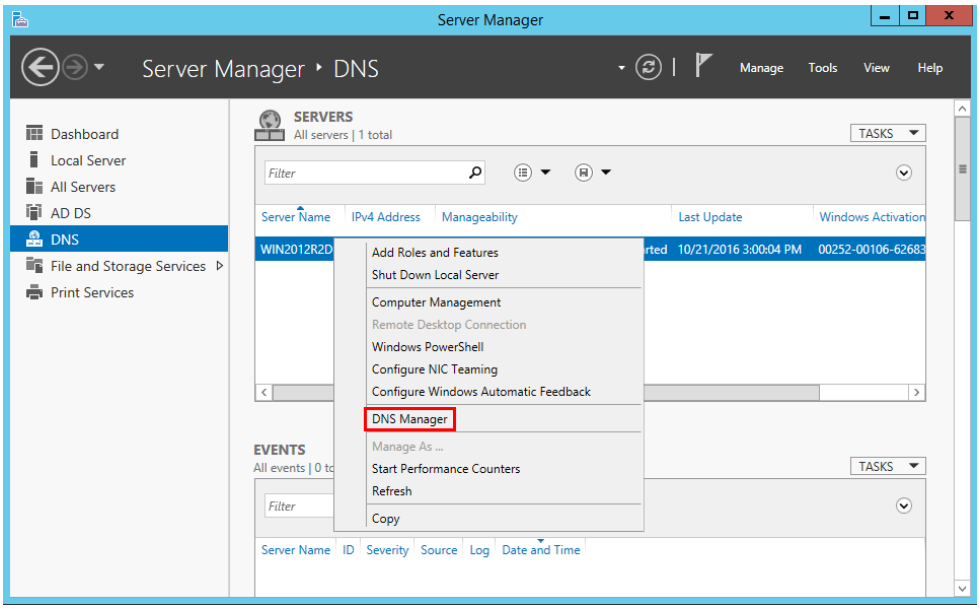
To create an alias, do the following:

1. On the DNS server, open the **Server Manager**.

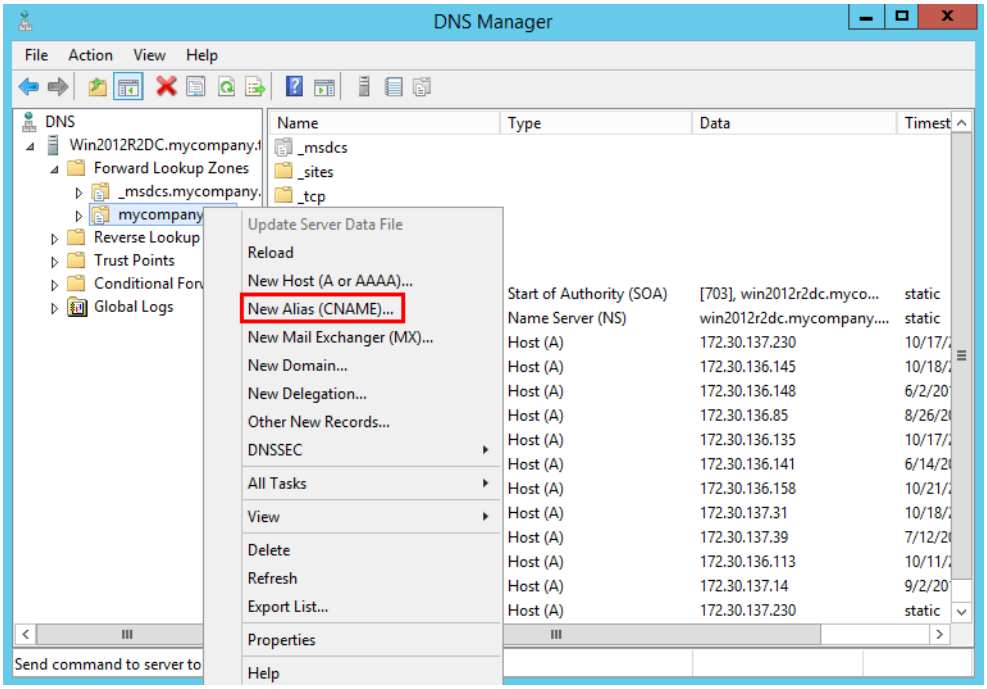
2. Click **DNS**.



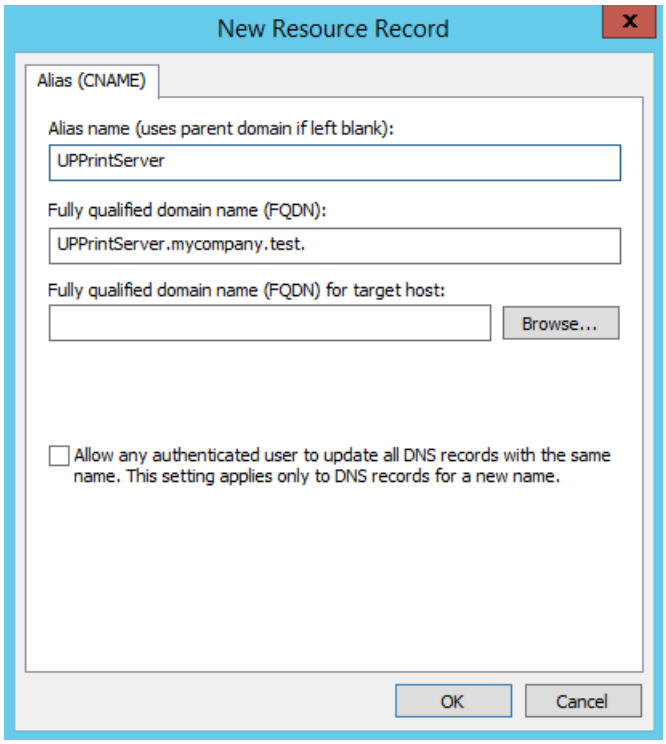
3. Right-click the DNS server name and then select **DNS Manager**.



4. In the **DNS Manager**, expand the server name and then expand the **Forward Lookup Zones**. Right-click the domain name and then select **New Alias (CNAME)**.

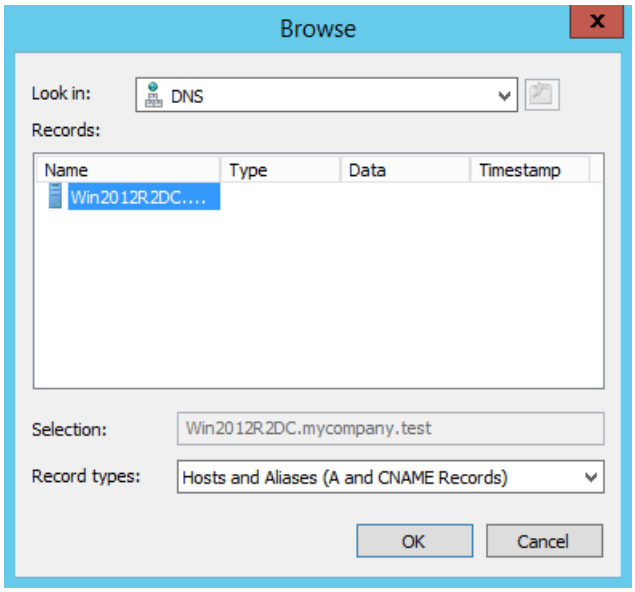


5. In the **New Resource Record** dialog box, under **Alias name (uses parent domain if left blank)**, type in **`UPPrintServer`**.

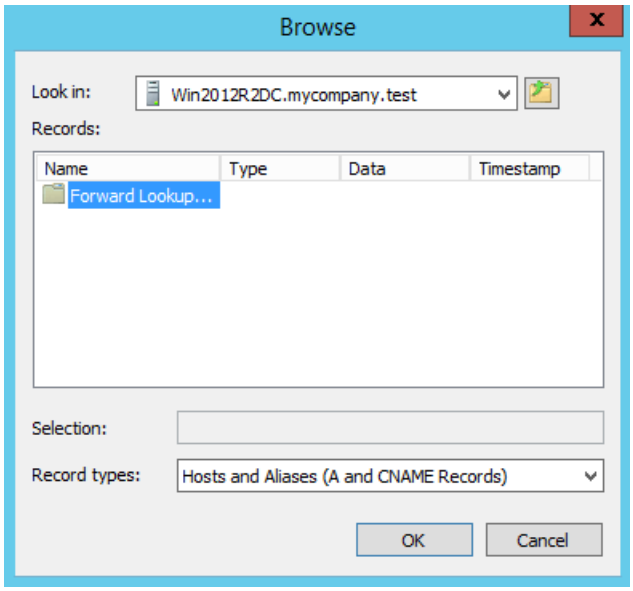


6. Beside **Fully qualified domain name (FQDN) for target host**, click **Browse**.

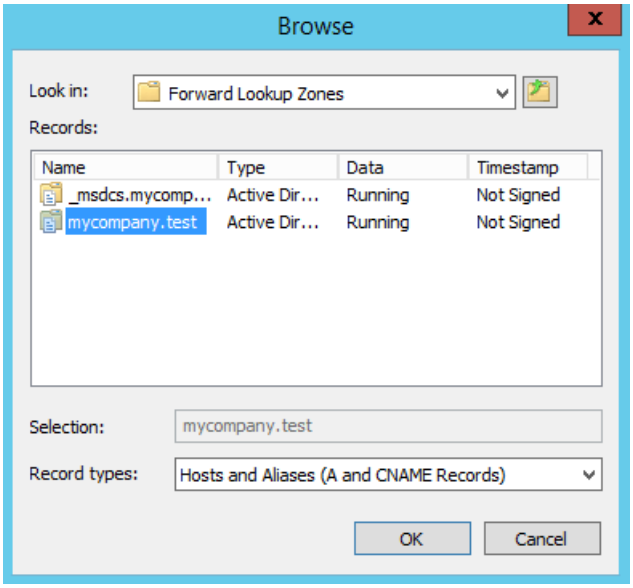
7. In the **Browse** dialog box, double-click the server name.



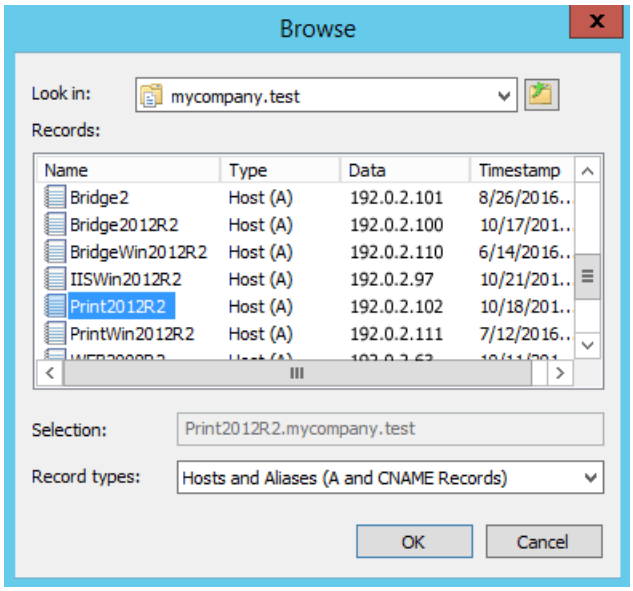
8. Double-click **Forward Lookup Zones**.



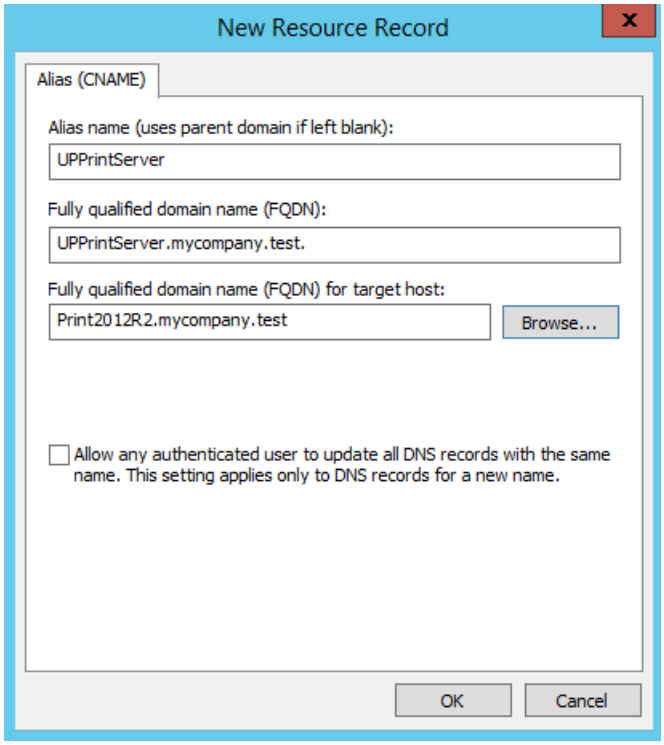
9. Double-click the domain name.



10. Under **Records**, click to select the print server host for which this alias is being created and then click **OK**.

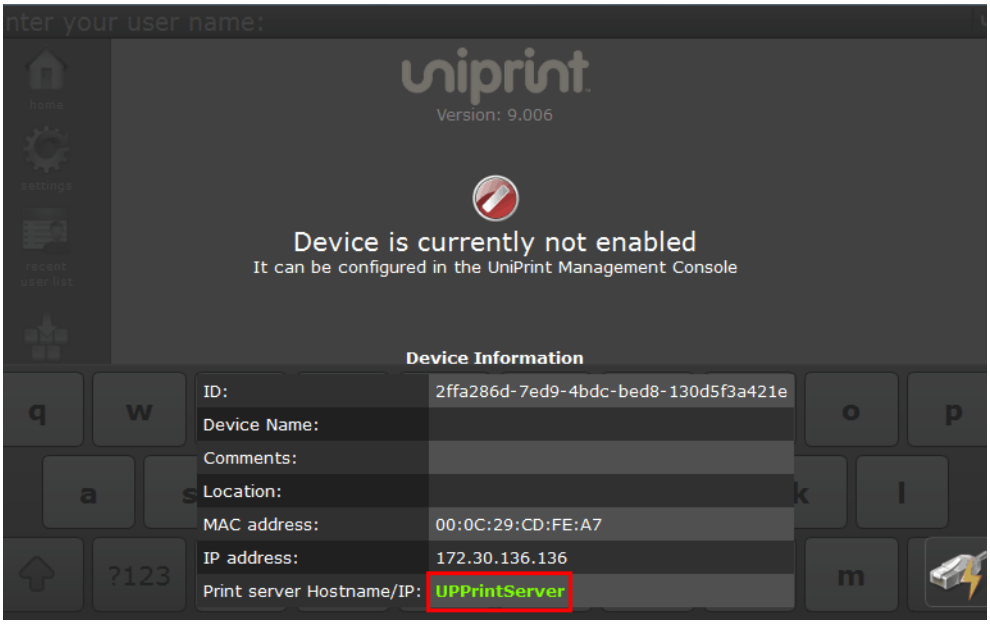


11. In the **New Resource Record** dialog box, click **OK**.



12. Restart the vPad Pro or vPad CE. To restart the vPad Pro, simply turn the power switch off and then turn it back on again. For the vPad CE

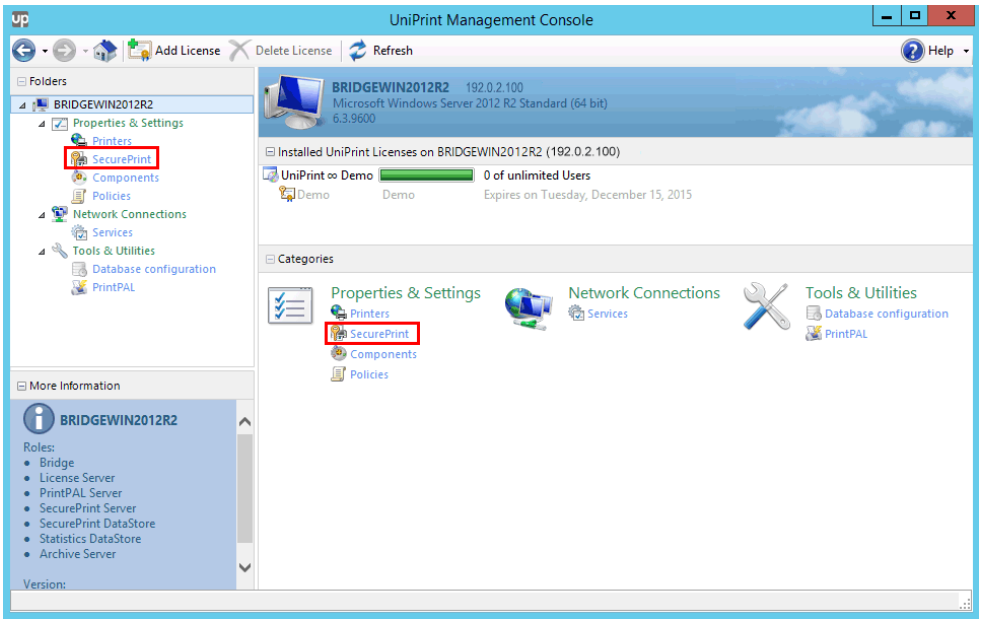
since it does not have a power switch, unplug the electrical cord and then plug it back in.



On the vPad Pro, a screen will appear with **UPPrintServer** as the **Print Server Hostname/IP**.

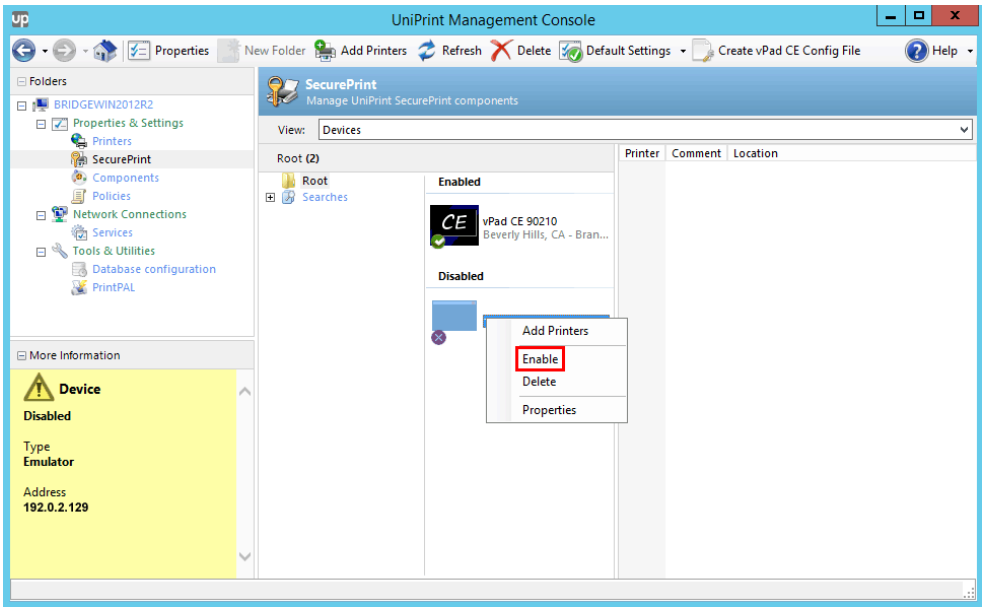
13. From a UniPrint component, open the **UniPrint Management Console**.

14. Under **Properties & Settings**, click **SecurePrint**.

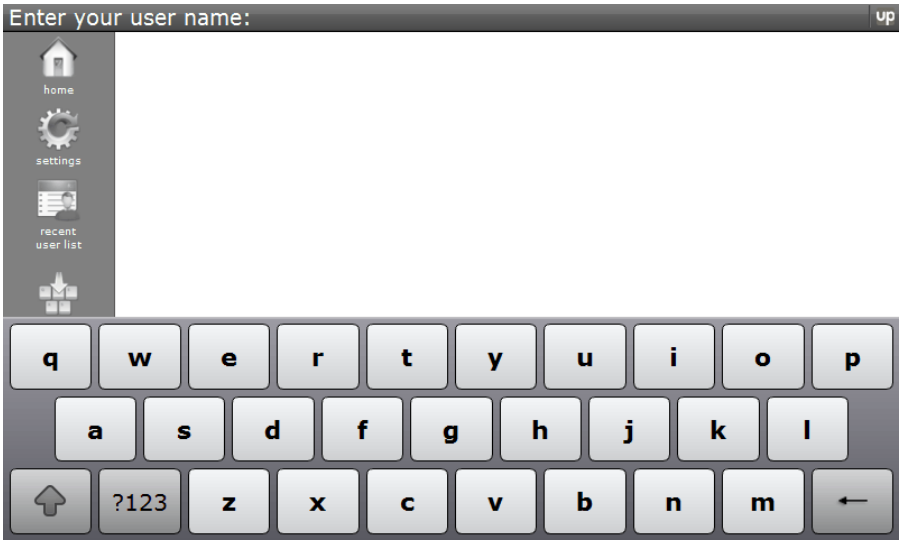


15. Click **Refresh** if the vPad does not immediately appear.

16. Right-click the vPad device and then select **Enable**.

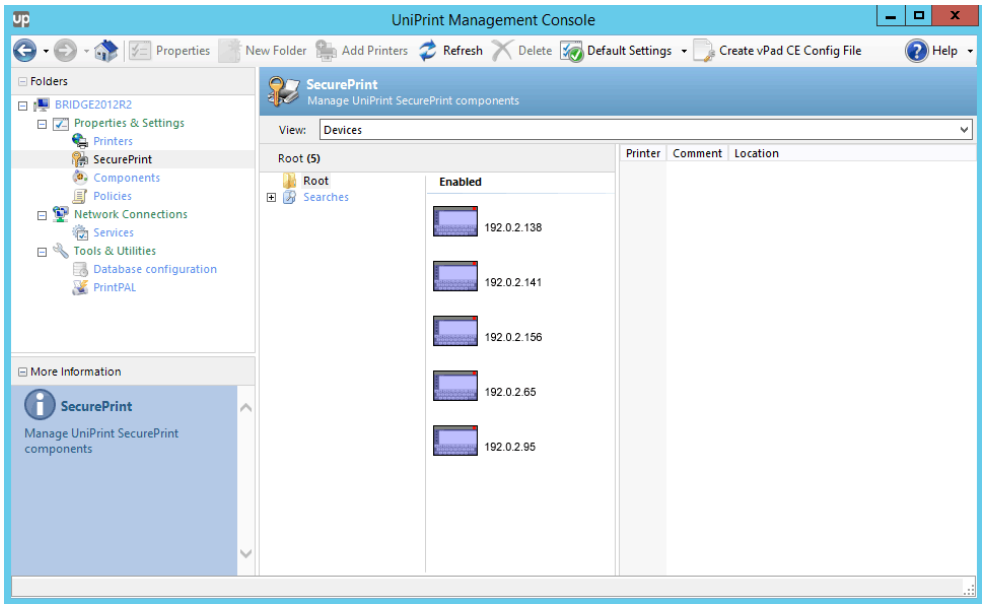


17. Once enabled, return to the vPad and the user name entry screen should appear.



Organizing Your vPads Using Folders

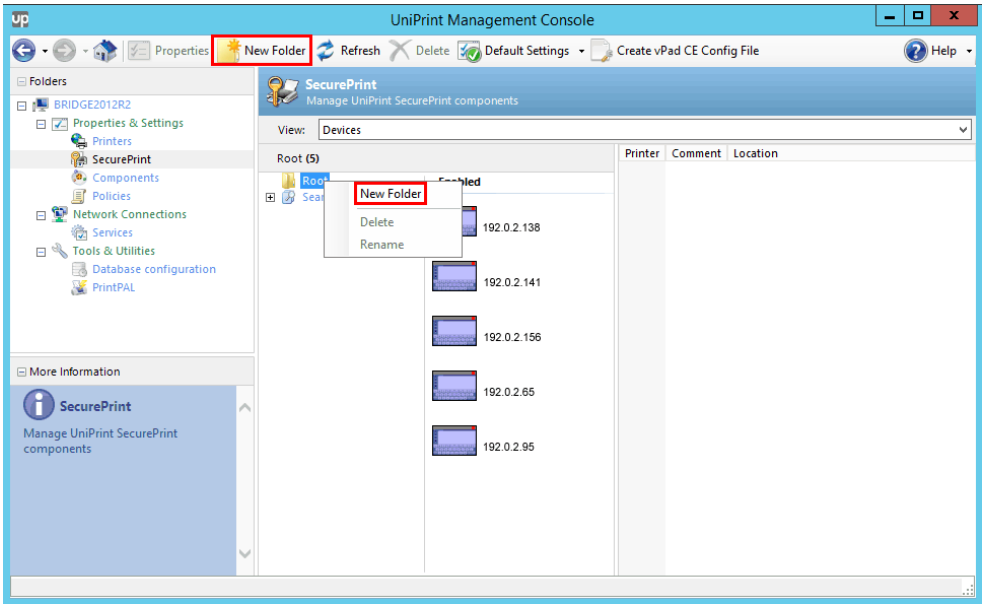
Initially, all vPads will be listed in the Root folder. Leaving all vPads there can be confusing especially when trying to locate a specific vPad. We suggest creating a folder structure to keep the vPads organized.



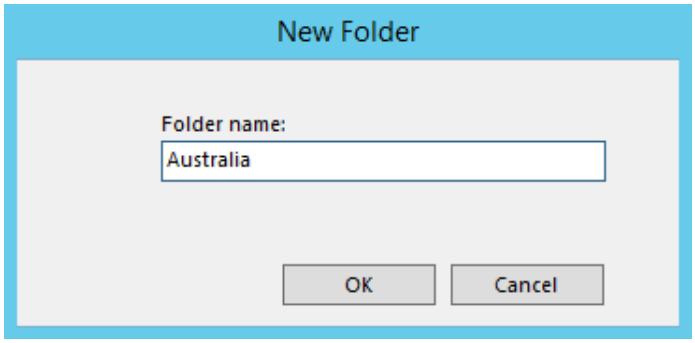
1. From a UniPrint component, open the **UniPrint Management Console**.

2. Under **Properties & Settings**, click **SecurePrint**

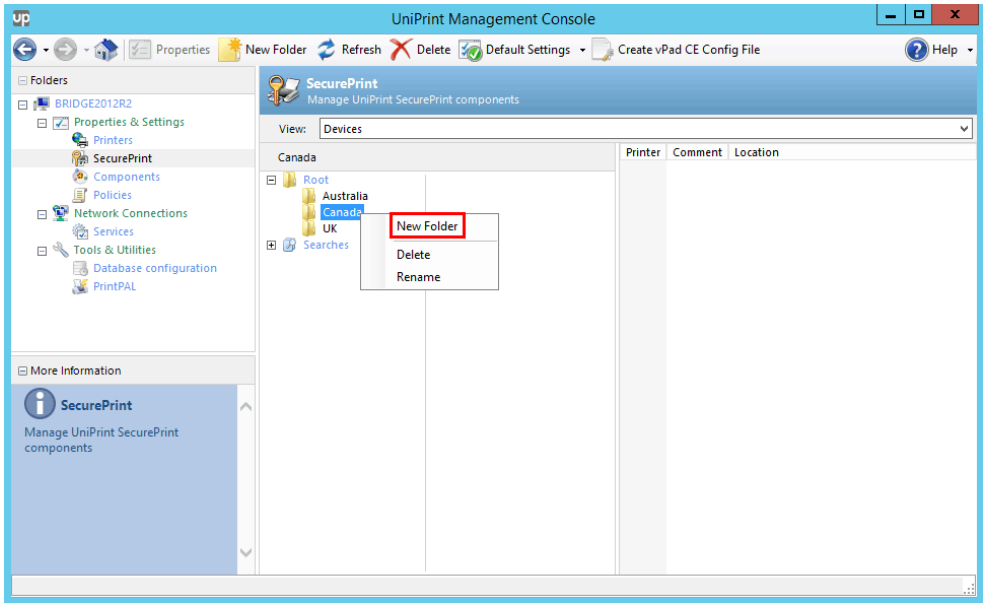
3. Click to select **Root** and then click **New Folder** or right-click **Root** and then select **New Folder**.



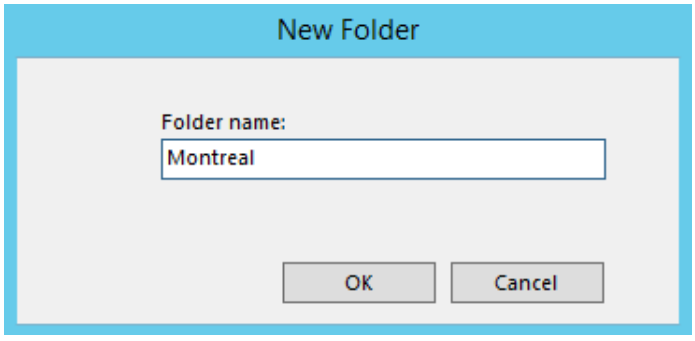
4. Enter the name of the new folder. Depending on your organization, this could be a region, city, division, campus, floor or department. Click **OK**.



5. To create a child folder, right-click the parent folder and then select **New Folder**.

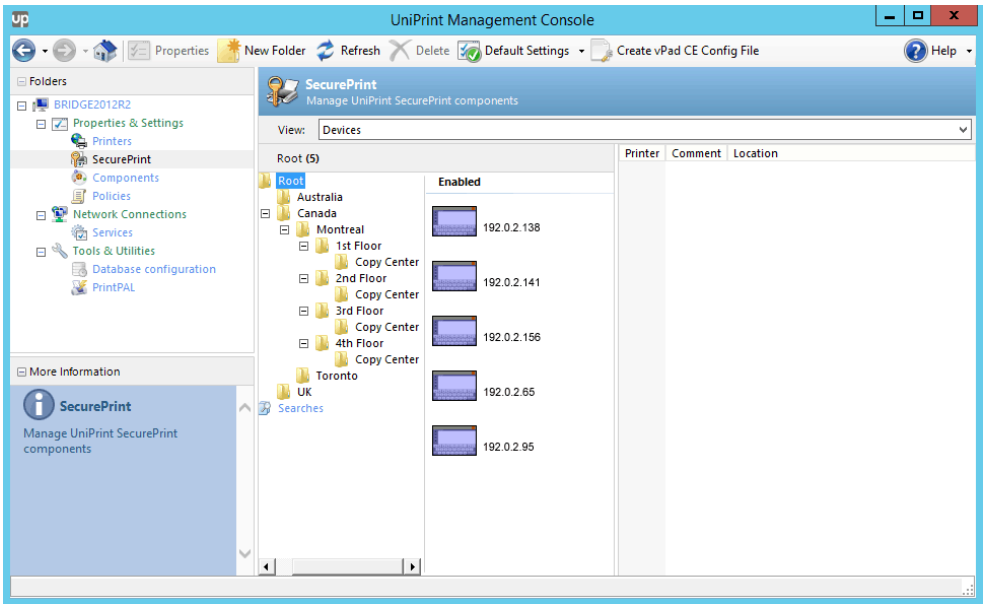


6. Enter the name of the new folder and then click **OK**.

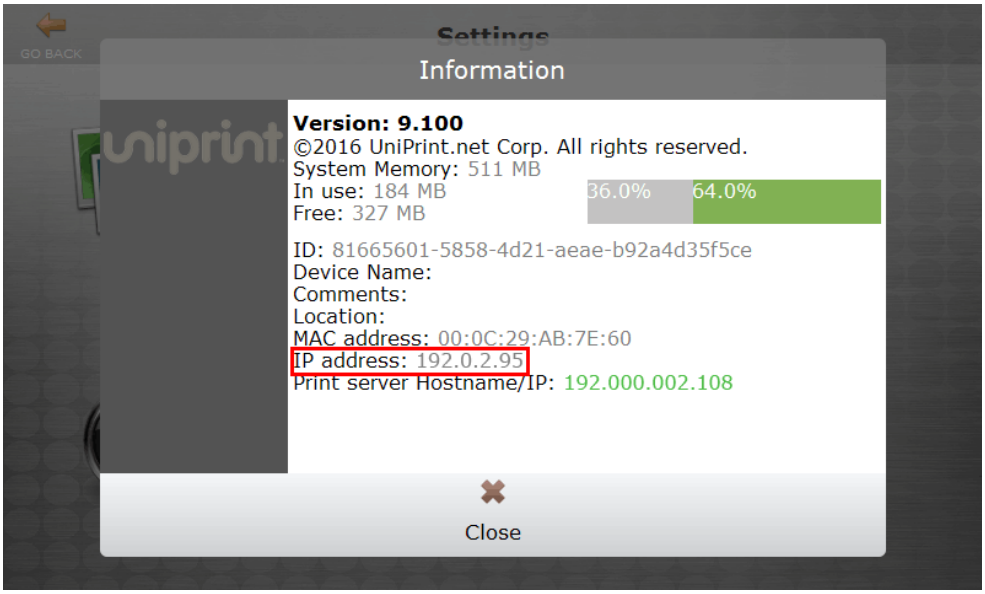


7. Continue creating folders as required.

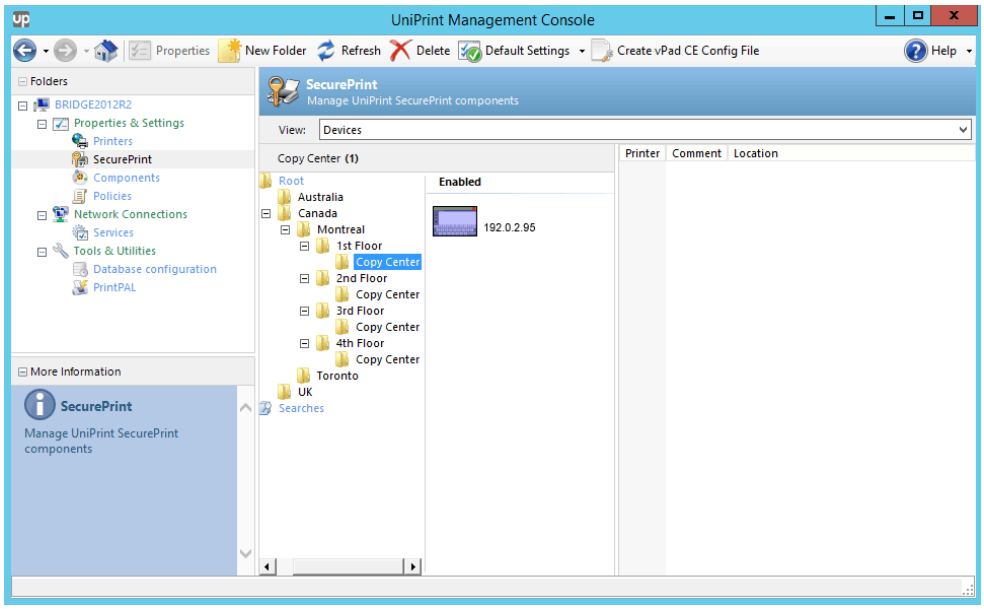
8. Click to select **Root** to view the vPads.



9. Determine which vPad belongs where in the tree by matching the vPad IP addresses. To determine the IP address of a vPad, at the vPad device, tap **Settings** and then tap **Information**.



10. Click and drag the vPad to the appropriate folder.



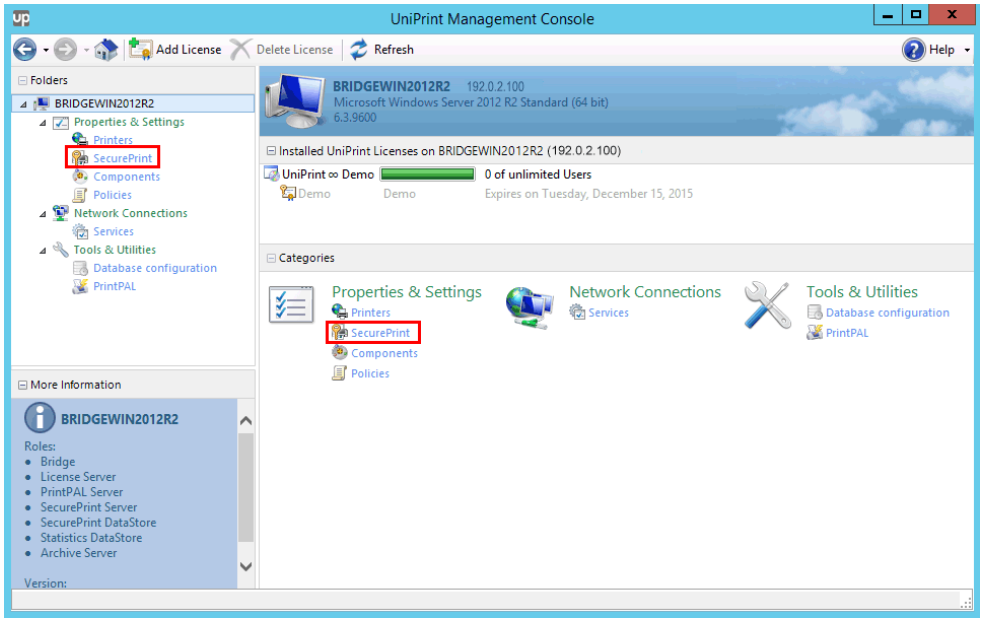
Changing SecurePrint Settings for A Single vPad Device

Initially, all vPads will be labelled with their IP address. Changing the settings, such as name, location and other settings will make this list more user friendly.

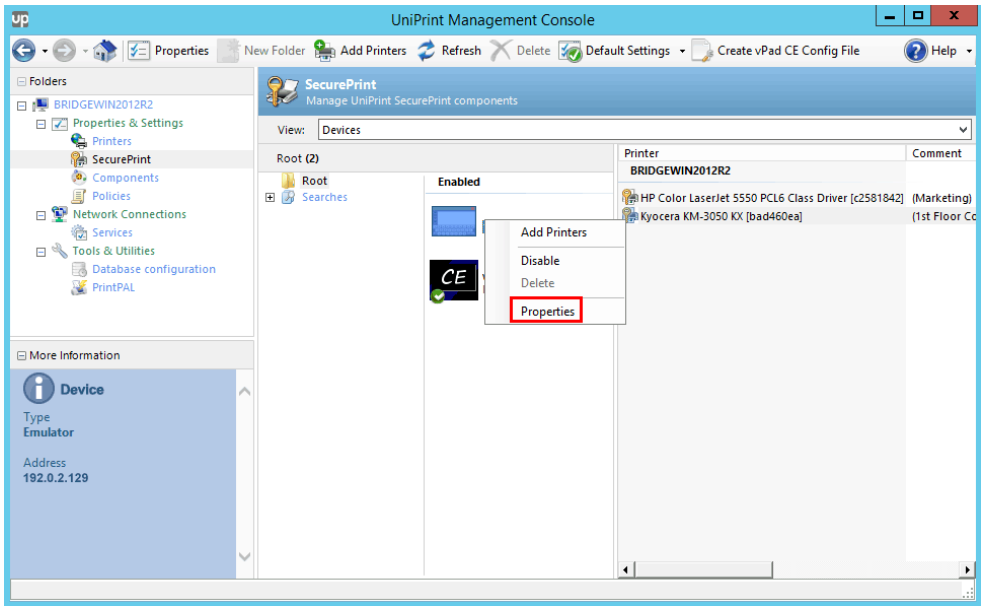
To edit the settings for a single vPad device, do the following:

1. From a UniPrint component, open the **UniPrint Management Console**.

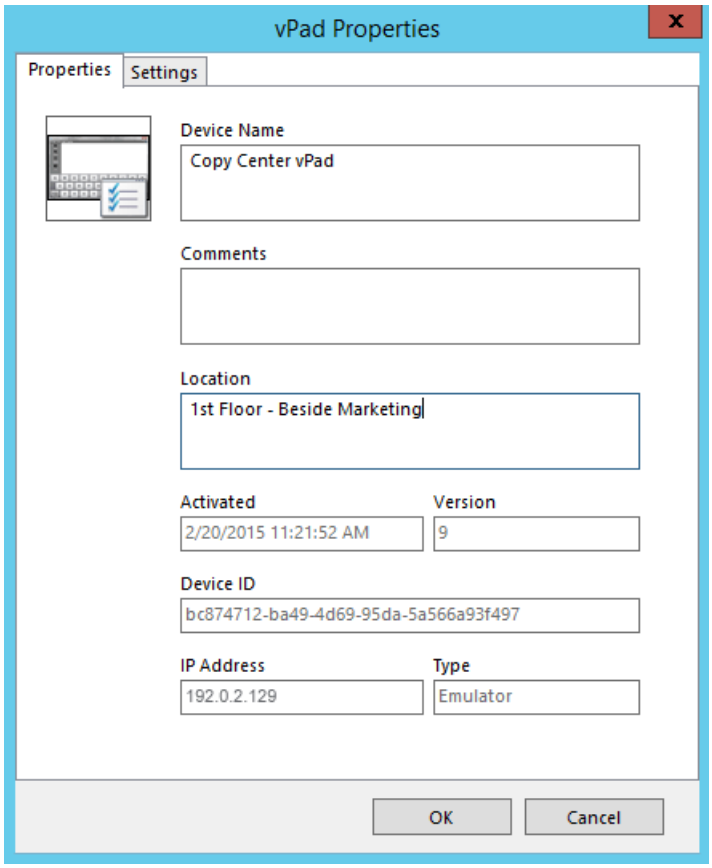
2. Under **Properties & Settings**, click **SecurePrint**.



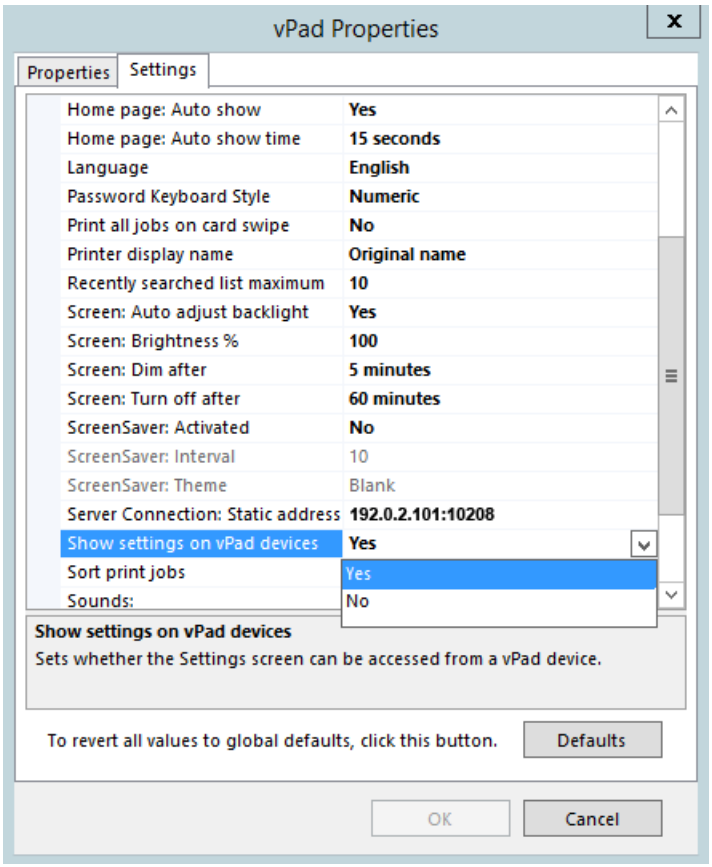
3. Right-click the device and then select **Properties**.



4. Enter in a **Device Name**, **Comments** and **Location** and then click the **Settings** tab. ***Note**: For vPad CE devices, only the **Device Name**, **Comment** and **Location** can be set.*



5. Change the desired settings and then click **OK**.



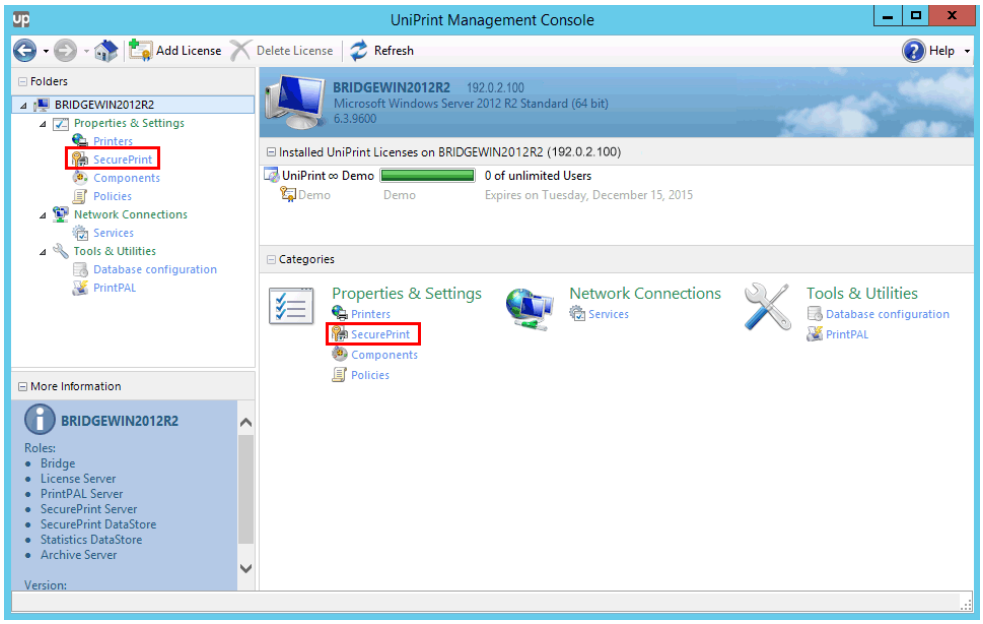
Changing SecurePrint Settings Globally for All vPad Devices

vPad device settings such as brightness, default home page and whether to show Settings on the device, and password settings such as Force Password can be applied to all devices through **Default Settings**.

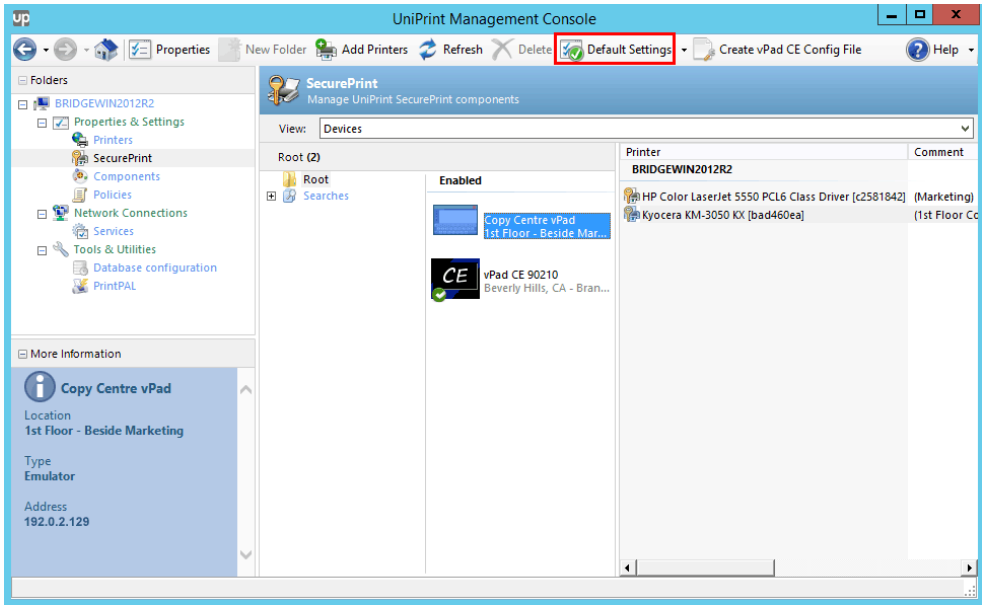
To edit settings for all vPad devices in your environment, do the following:

1. From a UniPrint component, open the **UniPrint Management Console**.

2. Under **Properties & Settings**, click **SecurePrint**.

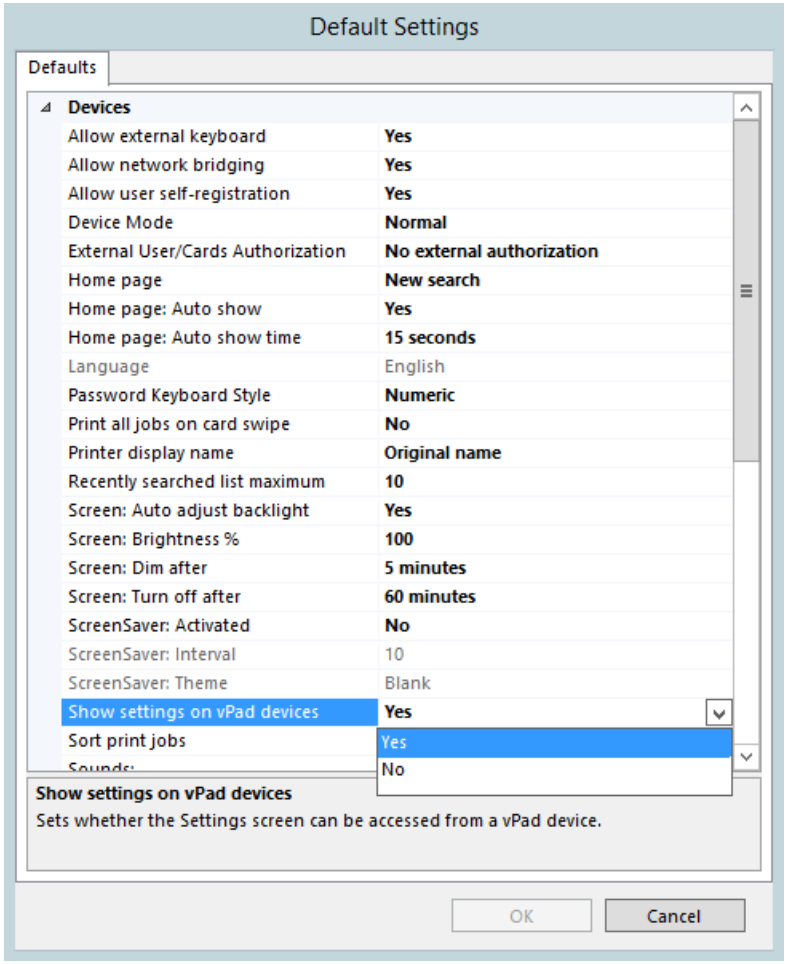


3. Click **Default Settings**.



4. Click to select the setting that you want to change and then select from the available parameter list. For example, to hide the **Settings**

button on the vPad, click to select **Show settings on vPad devices** and then select **No**.



5. Continue to change settings, referring to the table below and then click **OK** when done.

Setting	Description
Allow external keyboard	If set to **Yes**, then a USB keyboard can be attached to the vPad device. This setting does not apply to the SecurePrint Emulator. Default is **Yes**.
Allow network bridging	If set to **Yes**, then network bridging is permitted on this vPad device. This setting does not apply to the SecurePrint Emulator. Default is **Yes**.

Setting	Description
Allow user self-registration	If set to **Yes**, then after the user submits a print job with a password, the user can then register their contactless proximity smart card or a contact smart card with a magnetic strip through the vPad device in order to associate their user name to their smart card.
Delegated print job notification	If set to **Yes**, a notification bar will appear on the specified vPad device notifying users that a delegated print job is available for printing. The default is **Yes**.
Device Mode	Sets how users can retrieve print jobs from the vPad device. The options are Normal and Locked down. If set to **Locked down**, the device will be unresponsive to touch until a valid smart card or magnetic strip is used.
External User/Cards Authorization	Sets the external authorization method to be used for authentication. Third-party single sign-on and password management systems, such as Imprivata OneSign can be integrated into SecurePrint. The available options are: • **No external authorization** - Use a combination of domain username/ password or RFID/HID to access the vPad and then a print job specific SecurePrint password to release the print job. • **Imprivata with external reader** - Use an Imprivata proximity card on an external card reader to authenticate the user and release print jobs with a SecurePrint password. • **Imprivata with internal reader** - Use an Imprivata proximity card with the vPad internal card reader to authenticate the user and release print jobs with a SecurePrint password. Default setting is **No external authorization**.

Setting	Description
Home page	If set to **NewSearch**, users will be required to enter their user name in order to display their print jobs. If set to **RecentUserList**, users can scroll and select from a list of users who recently sent a print job, but have not retrieved it. **NewSearch** is the default Home page.
Home page: Auto show	If set to **Yes**, the default Home page will be displayed after a period of inactivity.
Home page: Auto show time	Sets the amount of time the vPad needs to be inactive before the screen changes to the default Home page. Available options are 15 seconds, 30 seconds, 1 minute, 2 minutes, and 5 minutes.
Language	English, French, German, Spanish, Italian, Polish and simplified Chinese interfaces are now available.
Password Keyboard Style	Sets the default keyboard style that appears when the user is prompted to enter their password. Available options are **Numeric** and **Alphabetic**. The default style is **Numeric**.
Print all jobs on card swipe	If set to **Yes**, all active print jobs are released to an assigned default printer when a card is swiped. If a default printer is not set, the user will be presented with a list of available printers.
Printer display name	Sets how printer names are displayed on the vPad. Available options are **Original name** and **UniPrint Gateway name**.
Recently searched list maximum	Sets the maximum number of user names displayed in the recently searched list.
Screen: Auto adjust backlight	If set to **Yes**, the screen will dim and then turn off automatically after a set amount of inactive time.
Screen: Brightness %	Sets the percentage of brightness. The default is 100%.

Setting	Description
Screen: Dim after	The vPad screen will dim, if it is inactive for the amount of time set here. Available options are 30 seconds, 1 minute, 2 minutes, 5 minutes, 10 minutes and 20 minutes.
Screen: Turn off after	The vPad screen will turn off, if it is inactive for the amount of time set here. Available options are 5, 10, 15, 20, 30, and 60 minutes.
ScreenSaver: Activated	If set to **Yes**, a screensaver will run on the vPad after a period of inactivity.
ScreenSaver: Interval	A screensaver will activate, if the vPad is inactive for the amount of time set here in seconds.
ScreenSaver: Theme	The theme can either be set **Blank** in which the screen turns off or to **Fading** where the UniPrint logo floats in different directions on the screen.
Server Connection: Static address:port	The static IP address and port number for the print server to which the vPad is connected can be added. ***Note**: The static IP address can only be set at the physical vPad device.*
Show settings on vPad devices	If set to **Yes**, the Settings icon and screen will be available on the vPad device and any user can change its settings.
Sort print jobs	Print jobs can either be displayed with the oldest first or the newest first.
Sounds	Tap sounds can be enabled or disabled.
Sounds: Volume	The volume can be set between 0 and 100%. The default is 50%.

Setting	Description
Spanning Tree Protocol (STP)	This setting is only applicable to the vPad device itself and does not apply to the Emulator. The vPad device has two network ports. One port should be connected to your network and the other port is intended to be connected to a network printer. However, if it is deemed necessary to connect both ports to the network, a bridge loop may be created resulting in broadcast radiation. To prevent this from occurring, set this setting to **On**. Default is **Off**.
Use Integrated Windows printer security	If set to **Yes**, SecurePrint will check Group Policies and display only the printers to which the user has access.
Cached jobs count	Sets the number of print jobs per user to keep cached in history. Default is 2.
Cached jobs expire	Sets whether cached jobs expire. If set to **Yes**, cached jobs will expire after the time set in **Cached jobs expire after**. If set to **No**, cached jobs never expire and will remain in the cached history until they are manually removed. Default is **Yes**.
Cached jobs expire after	Sets how long (in minutes) cached jobs are kept. Default is 14400 minutes (10 days).
Cached jobs expiry check	Sets how frequently (in minutes) the system checks for expired cached jobs. Default is 60 minutes.
Unclaimed jobs expire	Sets whether unclaimed jobs expire. If set to **Yes**, unclaimed jobs will be deleted after the time set in **Unclaimed jobs expire after**. If set to **No**, unclaimed jobs never expire and will remain in queue until they are manually deleted. Default is **No**.
Unclaimed jobs expire after	Sets how long (in minutes) unclaimed jobs are kept. Default is 1440 minutes. (24 hours).
Unclaimed jobs expiry check	Sets how frequently (in minutes) the system checks for unclaimed jobs. Default is 60 minutes.

Setting	Description
Require vPad password	If set to **Yes**, the user will be required to set and enter a password in order to release their print job.
Require VPQ password	If set to **Yes**, whenever the user prints to the UniPrint VPQ (virtual print queue), the user will be required to set and enter a password in order to release their print job.
Allow password bypass at device	This is for valid smart card, RFID or HID users. If set to **Yes**, only the smart card, RFID or HID is required for authentication and release of print jobs. If set to **No**, using the smart card, RFID or HID will only display the user's list of print jobs. However, the user will still be required to enter a password in order to release a print job.
Maximum print job password retry attempts	Sets the number of SecurePrint password attempts allowed on the vPad in order to release the print job. If the user exceeds the number of attempts set here, the print job is deleted and the user will have to print their document again and set another SecurePrint password. To set the number of attempts to unlimited, set this setting to 0. The default is 0.
User card limit	Sets the number of contactless/contact smart cards that can be associated to each user name.

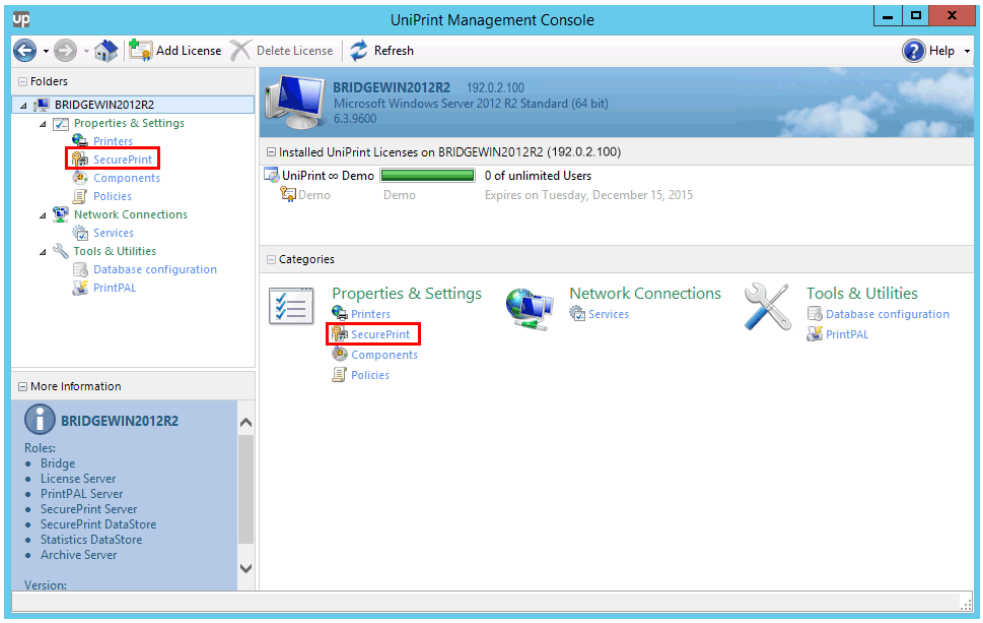
Adding Printers to the vPad

Each vPad can be used to release print jobs for one or more printers on the network. When adding a printer, you can force the user to enter a password.
***Note**: Printers do not need to be added to vPad CE devices.*

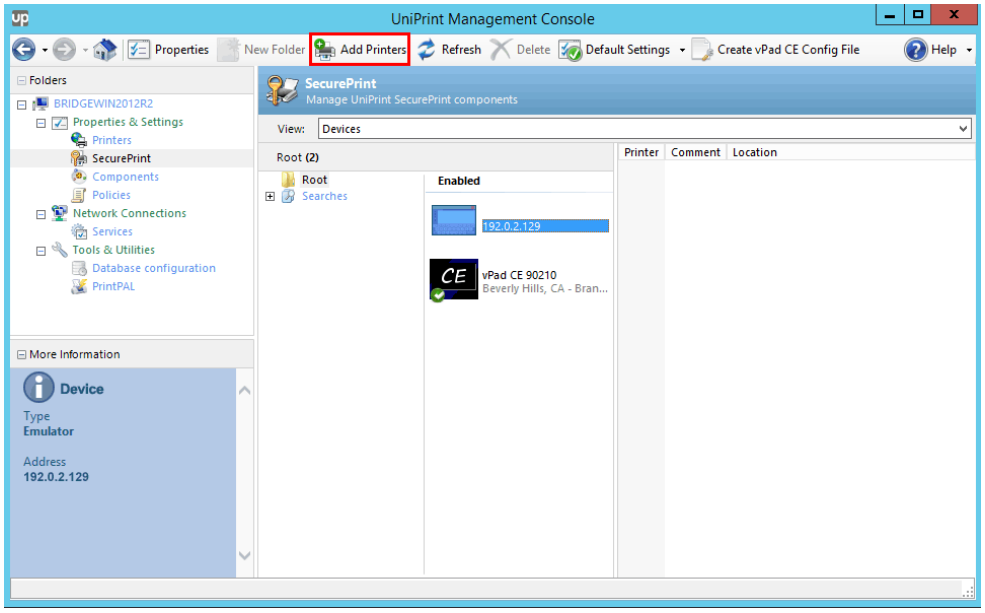
To add a printer to a vPad, do the following:

1. From a UniPrint component, open the **UniPrint Management Console**.

2. Under **Properties & Settings**, click **SecurePrint**.

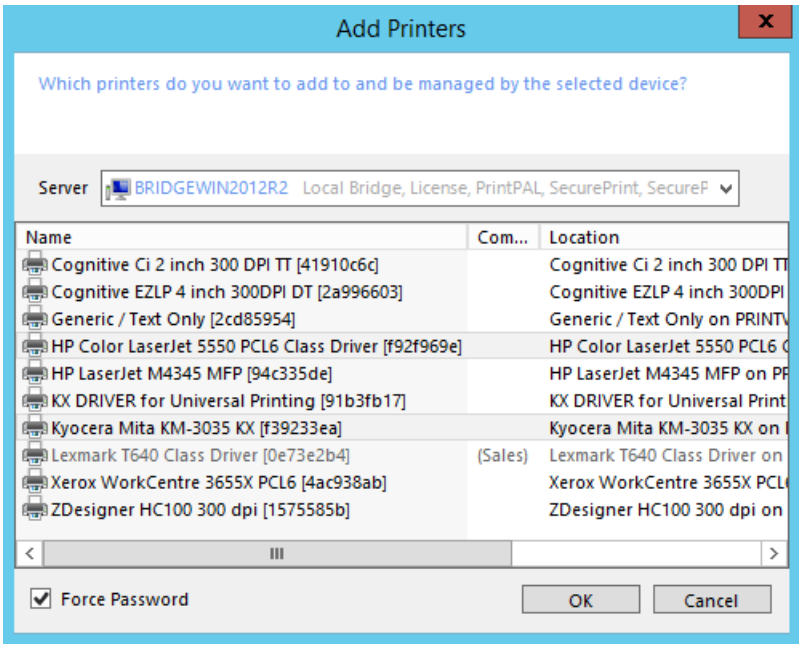


3. Click to select an enabled vPad and then click **Add Printers**.



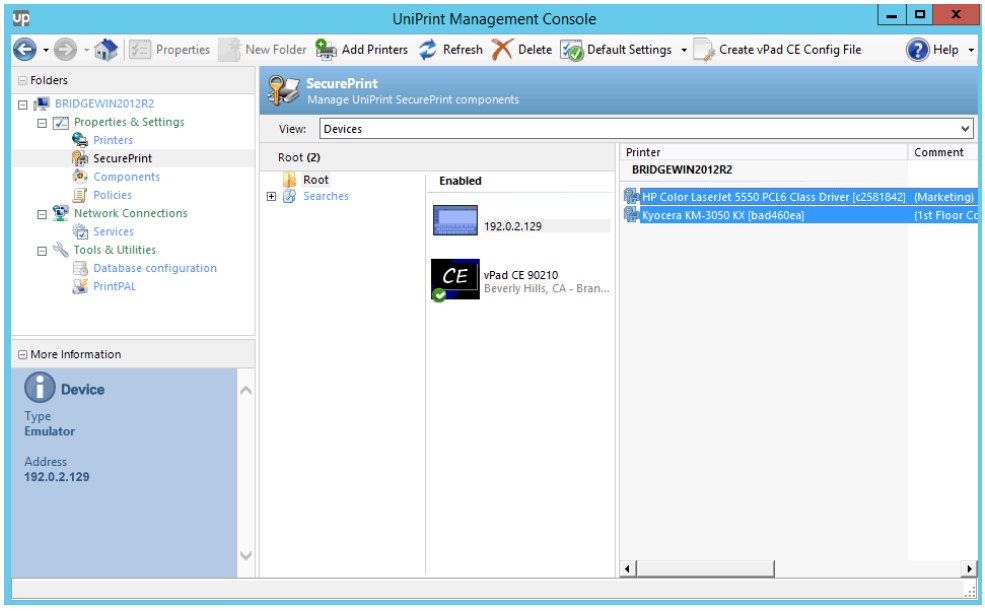
4. Click to select a printer and then select **Force Password** to make users enter a password in order to release their print job(s). ***Note**: To*

*select multiple printers, click to select a printer and then hold down the **SHIFT** key for consecutive printers or the **CTRL** key for non-consecutive printers.*



5. Click **OK**.

6. Repeat steps 4 to 5 to add more printers as required.



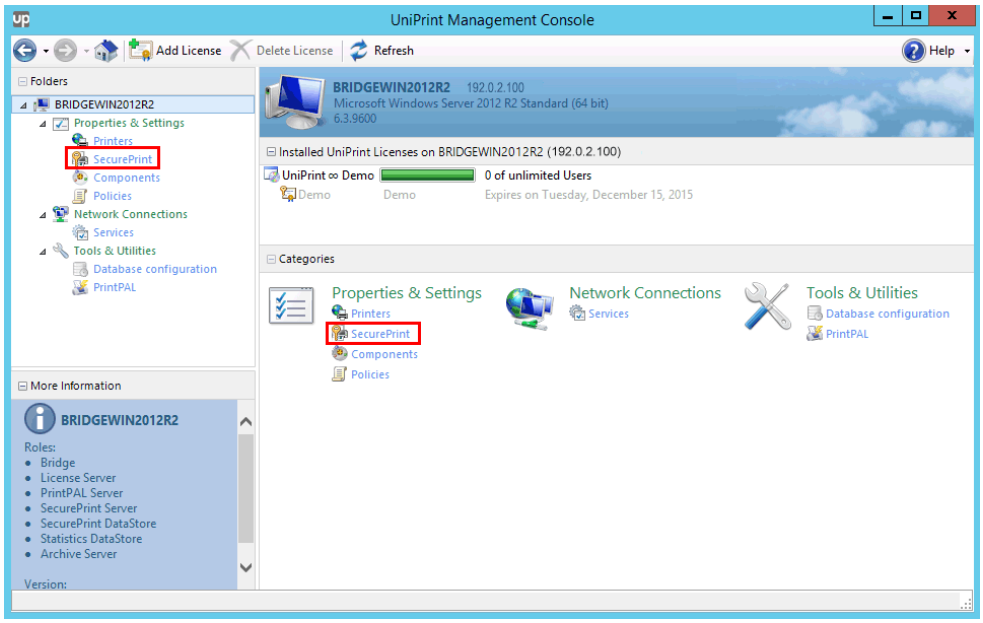
NOTE: If after a printer is added, hardware changes occur, such as, addition of trays or modules, the printer will need to be deleted on the UniPrint Management Console and then re-added in order for these hardware changes to be reflected when releasing print jobs.

Deleting a Printer from a vPad

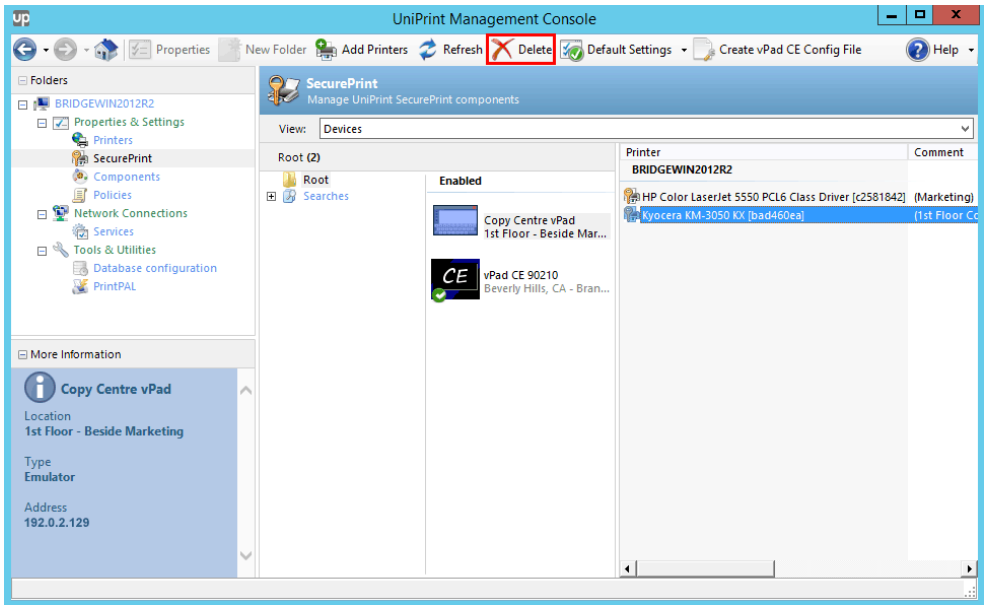
To delete a printer from a vPad, do the following:

1. From a UniPrint component, open the **UniPrint Management Console**.

2. Under **Properties & Settings**, click **SecurePrint**.



3. Click to select a printer to delete and then click **Delete**.



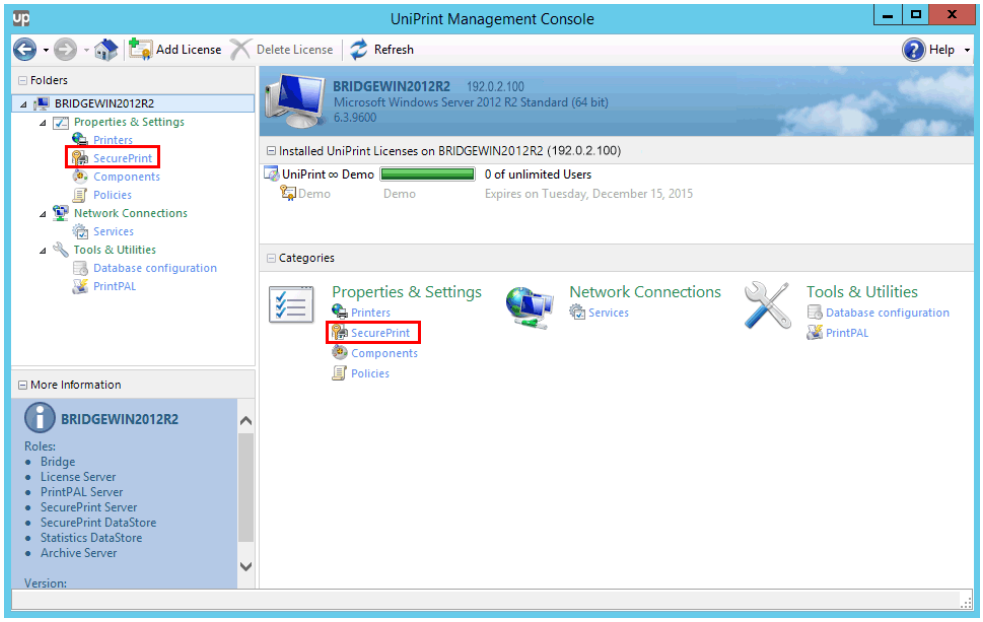
4. Click **Yes** to confirm that you want to delete this printer.

Disabling the Force Password option on a printer

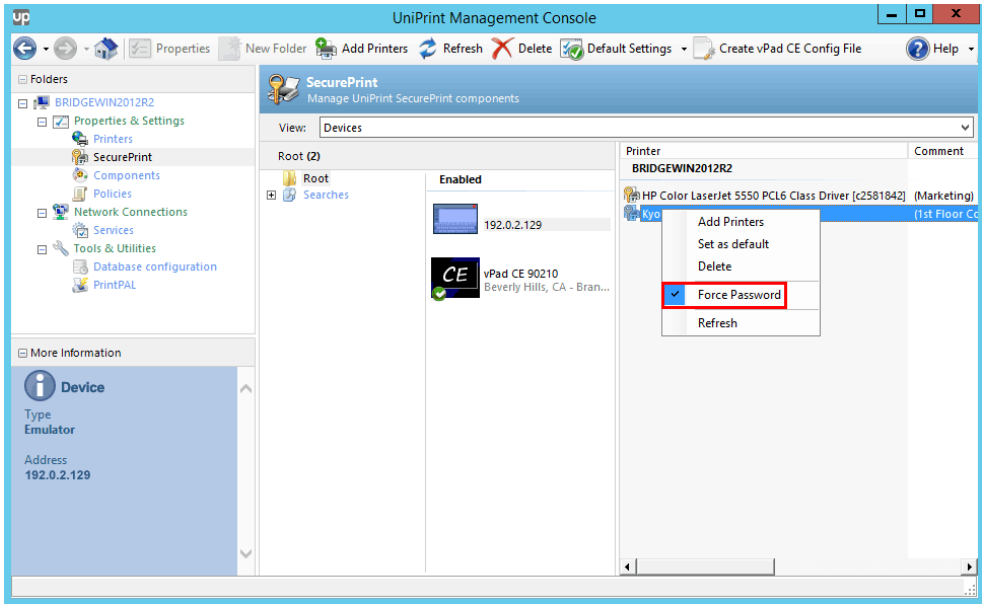
If you don't want to force your users to enter a password, then do the following:

1. From a UniPrint component, open the **UniPrint Management Console**.

2. Under **Properties & Settings**, click **SecurePrint**.



3. Right-click the printer that you want to remove the Force Password option from and then select **Force Password**.



4. The golden key will be removed from the printer icon to indicate that this printer no longer requires a SecurePrint password in order to release print jobs.

Associating A Smart Card With A User Name

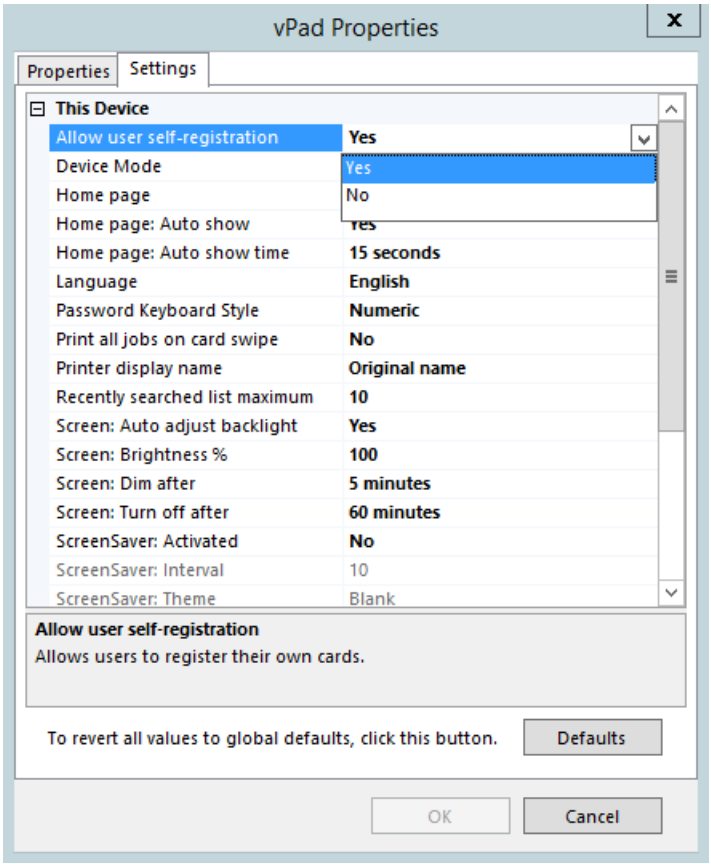
Before a user can associate their smart card directly at the vPad, the network administrator must first enable this functionality on the UniPrint Management Console.

1. On a UniPrint component, open the **UniPrint Management Console**.

2. Under **Properties & Settings**, click **SecurePrint**.

3. Click to select an individual vPad and then click **Properties**.

4. Set **Allow user self-registration** to **Yes**.



Users can register their smart card at the vPad, by doing the following:

1. Print a document to a UniPrint Gateway printer or UniPrint VPQ with SecurePrint password enabled. See "Setting up your SecurePrint Password" on page 304.

2. At the vPad, swipe, wave or tap the user's smart card or proximity ID.

3. A message will appear informing you that the proximity ID has not yet been associated with a user name. To continue and associate the ID with the user name, click **OK**.

4. Search and then select a user name.

5. Enter the SecurePrint password set in step 1 and then click **OK**. The proximity ID is now associated with the user name and the print job can now be released.

Disabling and Removing an Associated Smart Card From SecurePrint

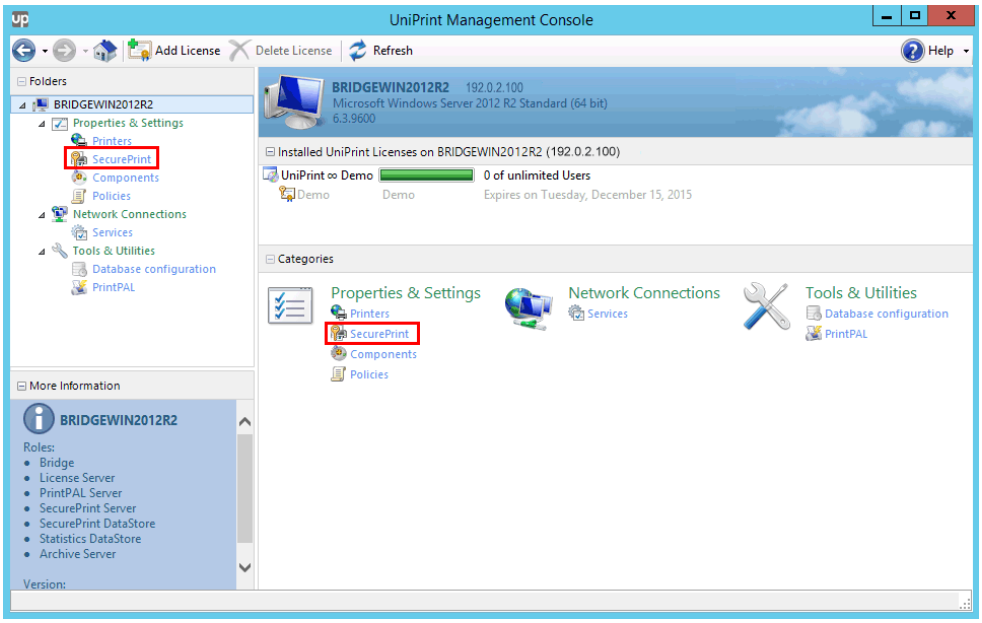
Although users can associate their smart cards to their domain user names through self-registration on the vPad, removing their proximity IDs from the SecurePrint database can only be done by the Administrator.

If a user loses their smart card or proximity ID, the card can be disabled temporarily or it can be deleted altogether. A new ID can then be issued and the user can be registered again in SecurePrint.

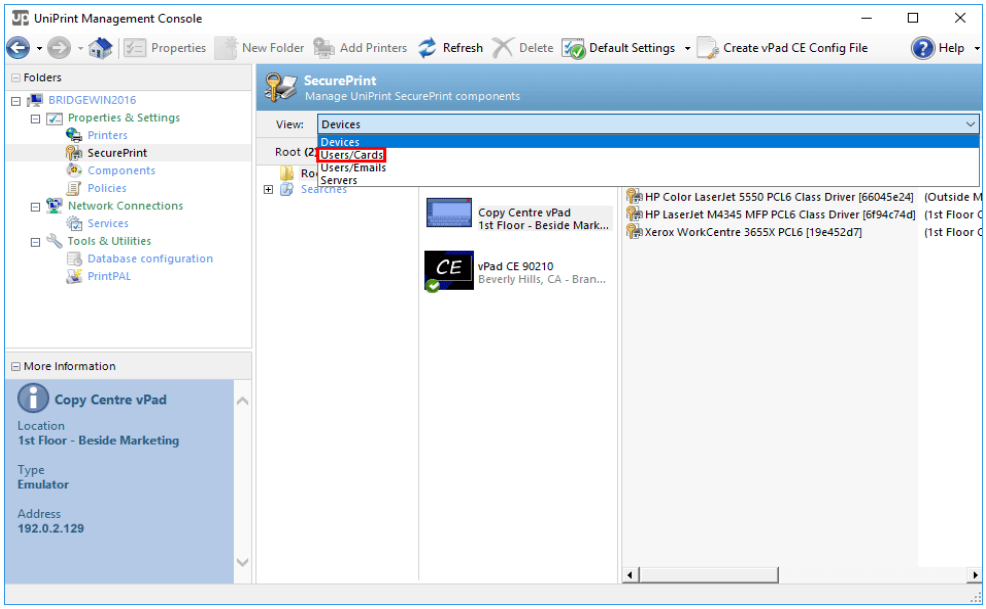
To disable or remove an associated smart card, do the following:

1. From a UniPrint component, open the **UniPrint Management Console**.

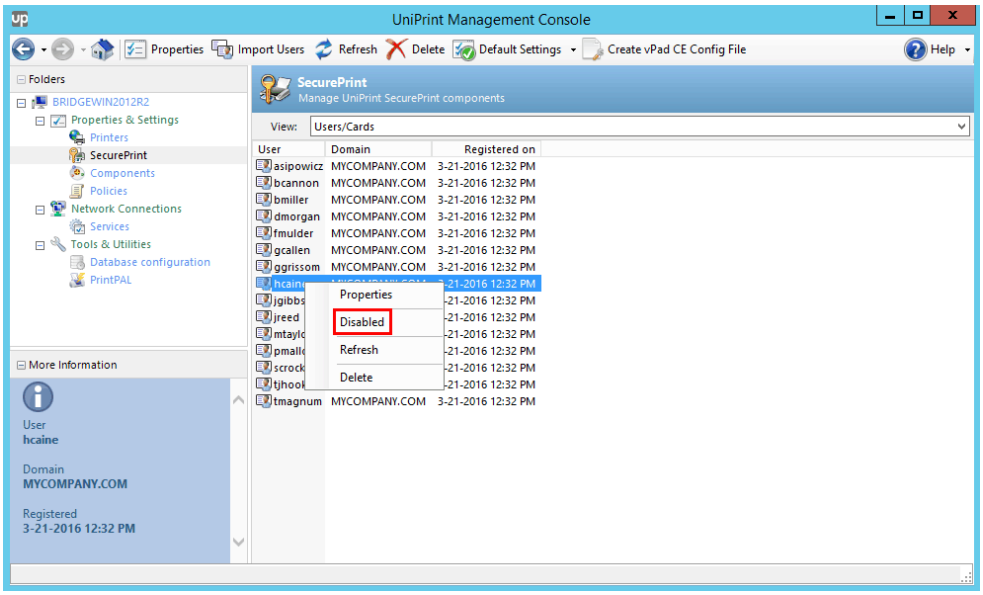
2. Under **Properties & Settings**, click **SecurePrint**.



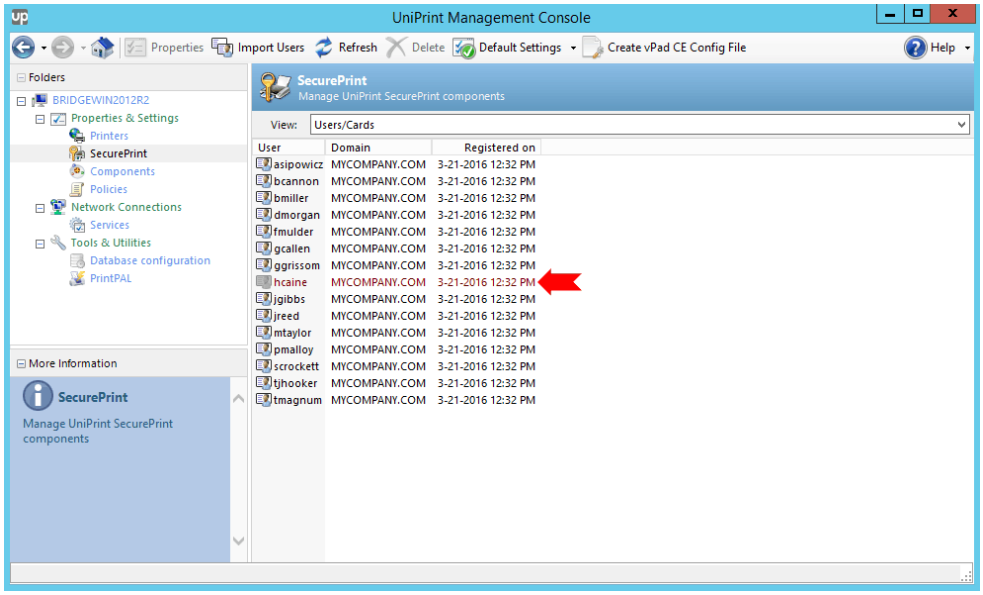
3. From the **View** list, select **Users/Cards**.



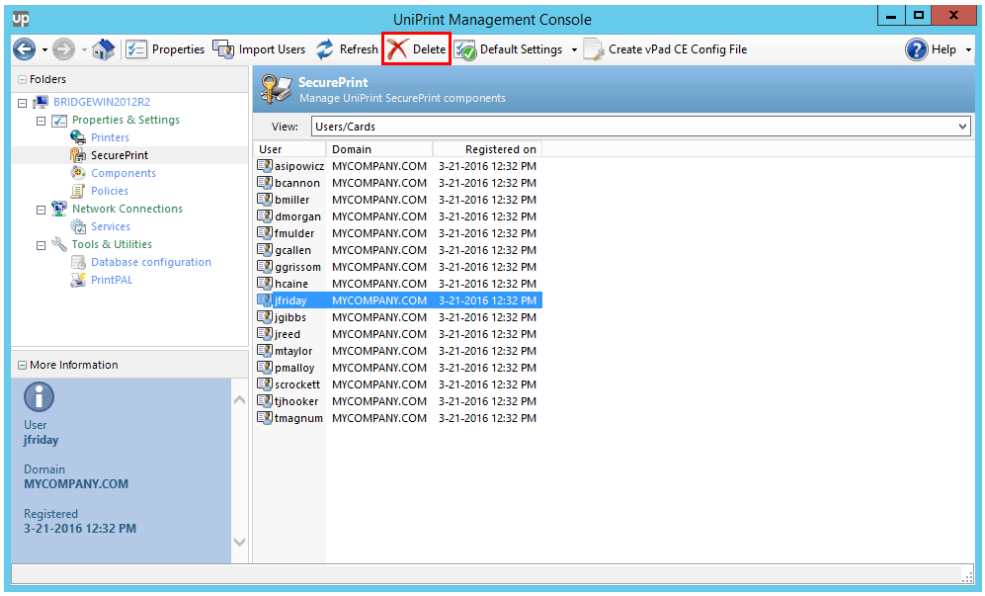
4. To disable a user card, right-click the user name and then select **Disabled**.



a. The disabled user name will turn red.



5. To remove a user card, click to select a user name and then click **Delete**.



6. Click **Yes** to confirm that you want to delete the selected user card. The user card will be removed from the list.

Importing A List Of Users and Smart Card IDs Into SecurePrint

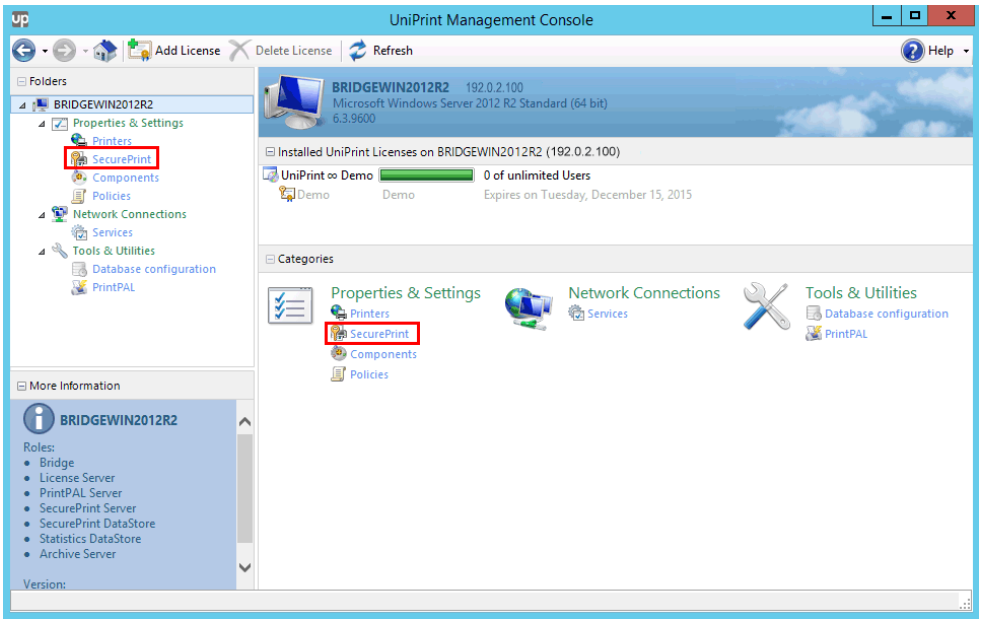
An alternative to having your users register their smart card/proximity IDs individually on each vPad, is to import a list of users. To do this, a user and ID number list must first be created. The list must have the user name, domain and ID number which can either be delimited with commas, spaces, semicolons or tabs and be saved either as a text (.txt) file or comma delimited file (.csv). The domain can be omitted, if all of your users belong to the same domain.

NOTE: When creating the list of users and ID numbers, ensure that spaces are not added after commas or semicolons, if they are used as delimiters.

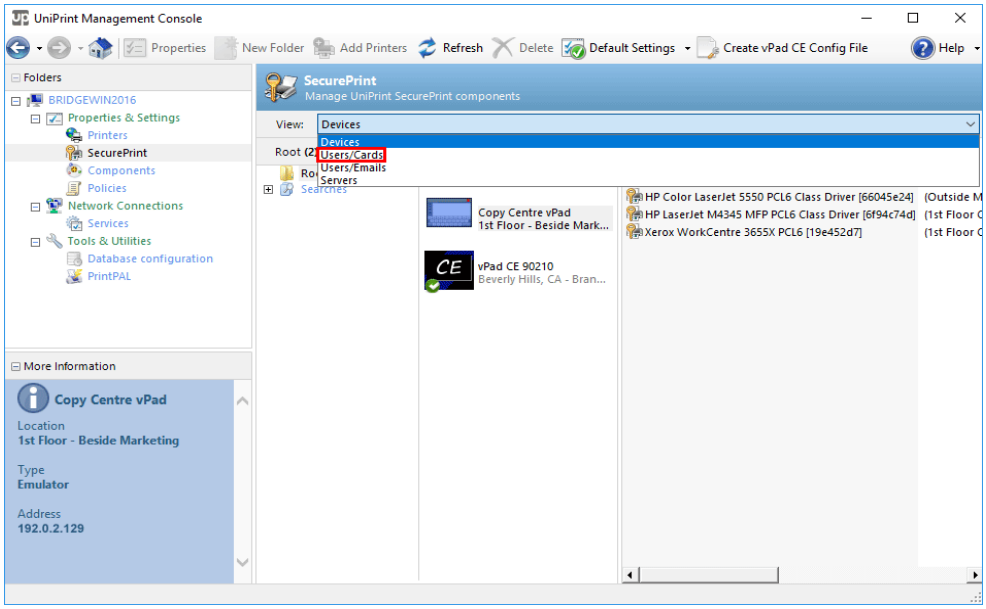
After creating your user list, follow these steps to import the data into SecurePrint:

1. From a UniPrint component, open the **UniPrint Management Console**.

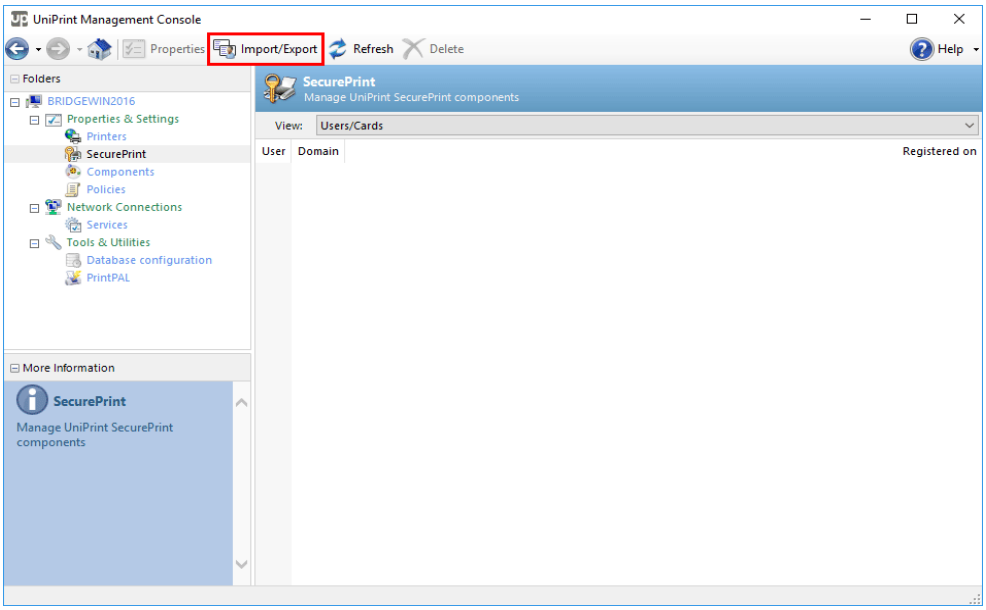
2. Under **Properties & Settings**, click **SecurePrint**.



3. From the **View** list, select **Users/Cards**.

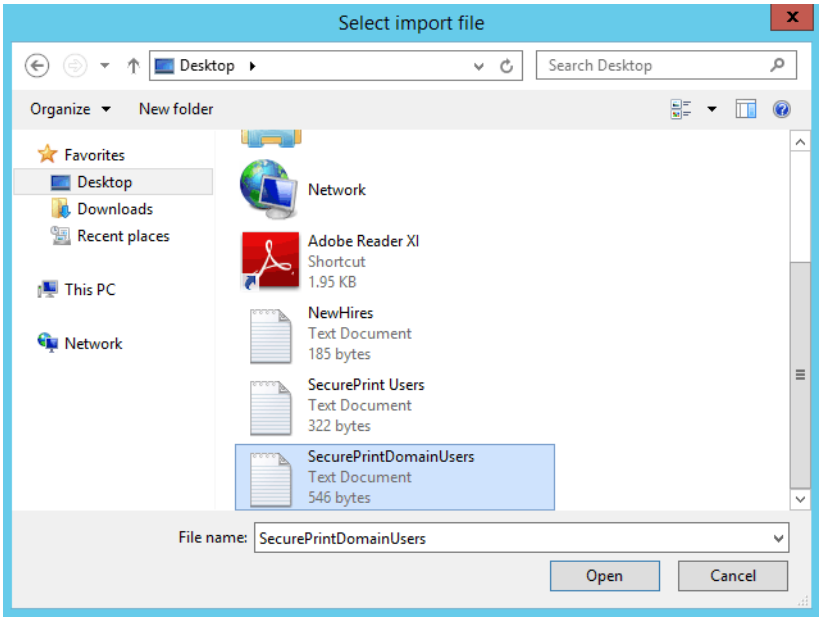


4. Click **Import Users**.



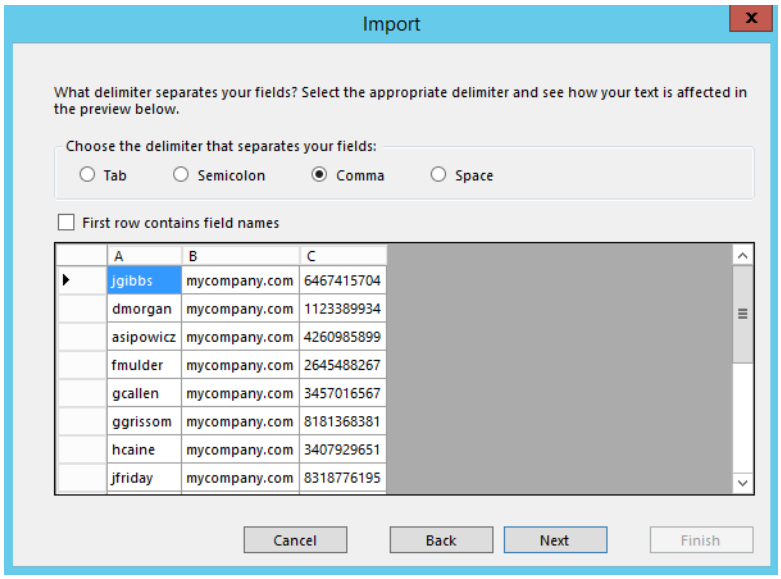
5. Click **Browse** to locate the user list that you created.

6. Click to select the user list and then click **Open**.

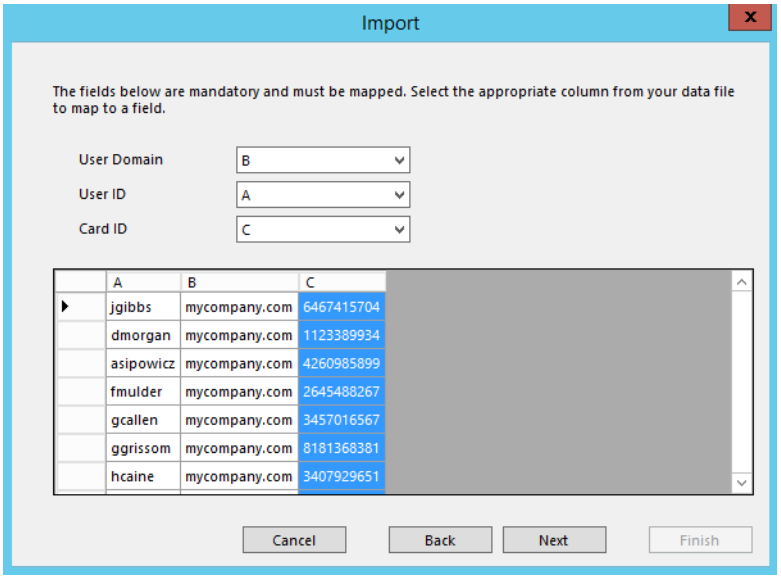


7. Click **Next**.

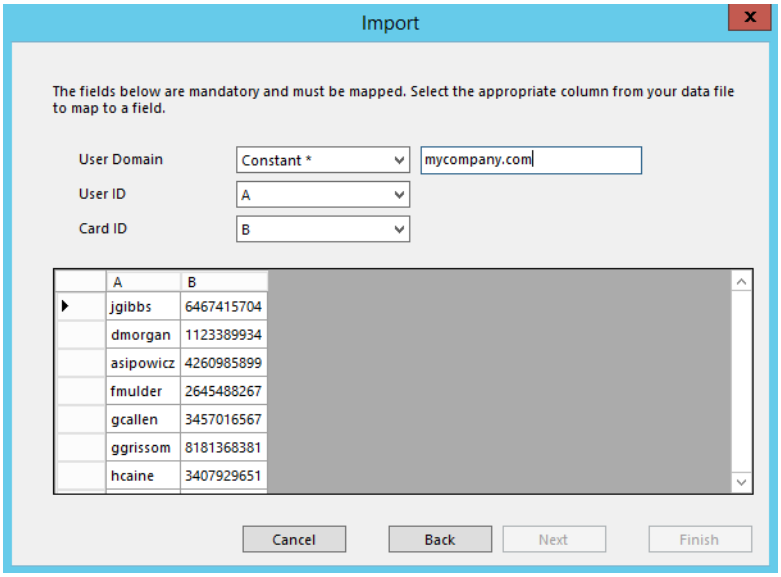
8. Select the type of delimiter used in the file and then click **Next**.



9. Map the appropriate columns to the data and then click **Next**.

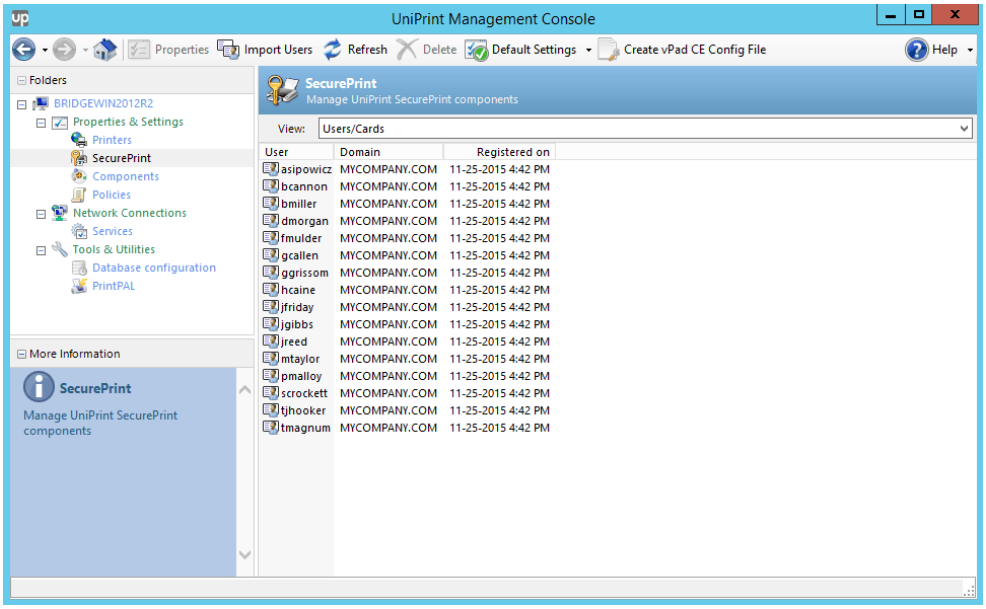


a) If no domain is specified, select **Constant** and then enter the domain.



10. Click **Next** and then click **Finish**.

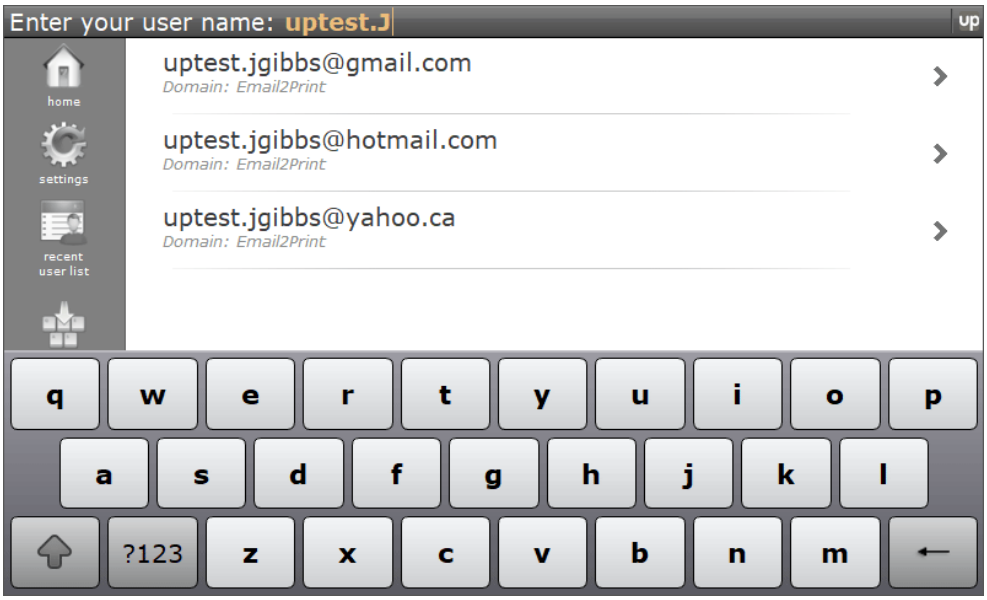
The imported user and card information will appear on the console.



Associating Many E-mail Addresses to One Domain User Name

With Email2Print, a user can print from any e-mail address as long as they know the e-mail address of the intended Gateway printer or the UniPrint VPQ. In earlier versions of SecurePrint, to release an Email2Print job at the vPad device, the user was required to enter the e-mail address that originally

sent the print job. Including their corporate e-mail account and web mail addresses, a user could have many e-mail accounts.



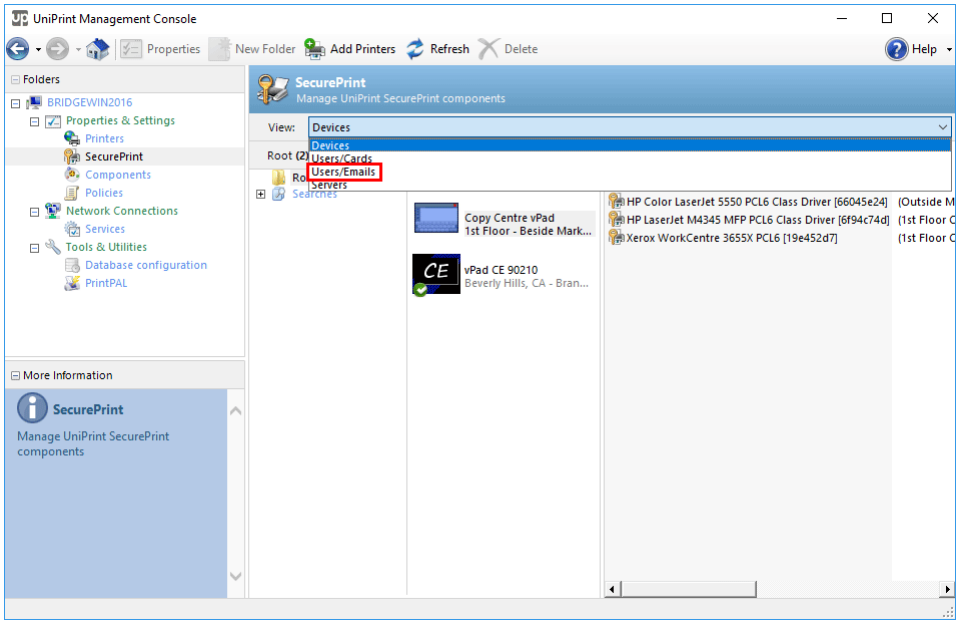
User Replacement Mapping enables users to enter their domain user name and all of their print jobs from all of their e-mail accounts and even their in-session print jobs will appear under their domain user name. The user no longer needs to go into each e-mail address in order to release their print jobs.

To associate many e-mail addresses to one domain user name, do the following:

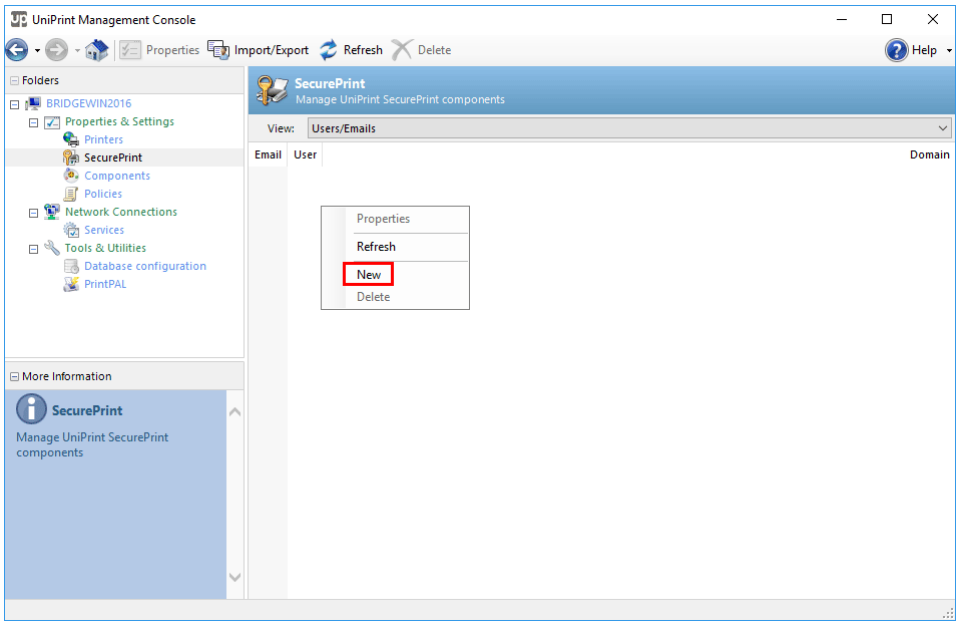
1. On the SecurePrint Server (UniPrint Bridge), open the **UniPrint Management Console**.

2. Under **Properties & Settings**, click **SecurePrint**.

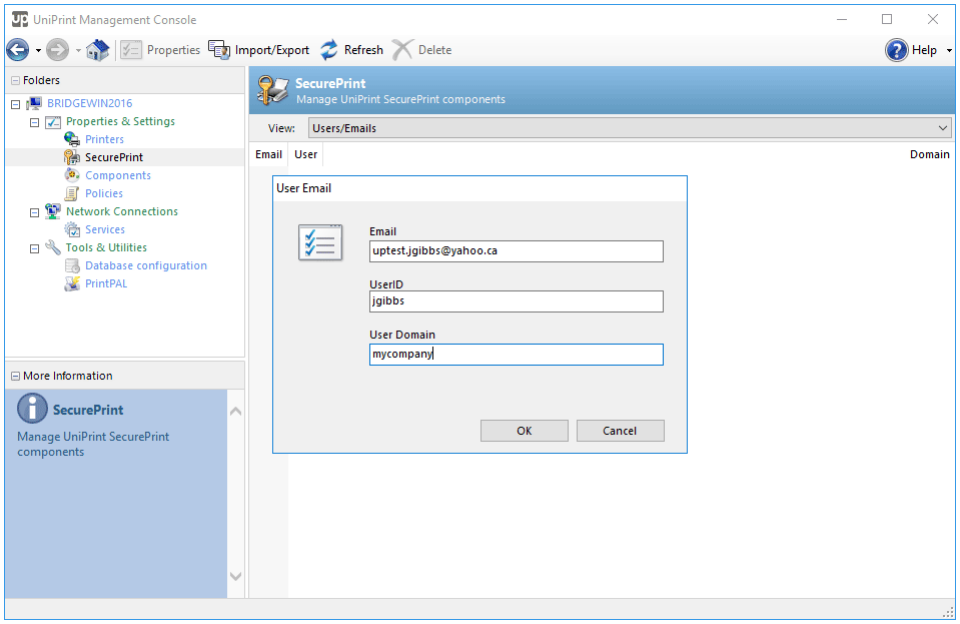
3. From the **View** list, select **Users/Emails**.



4. Right-click in the window and then select **New**.

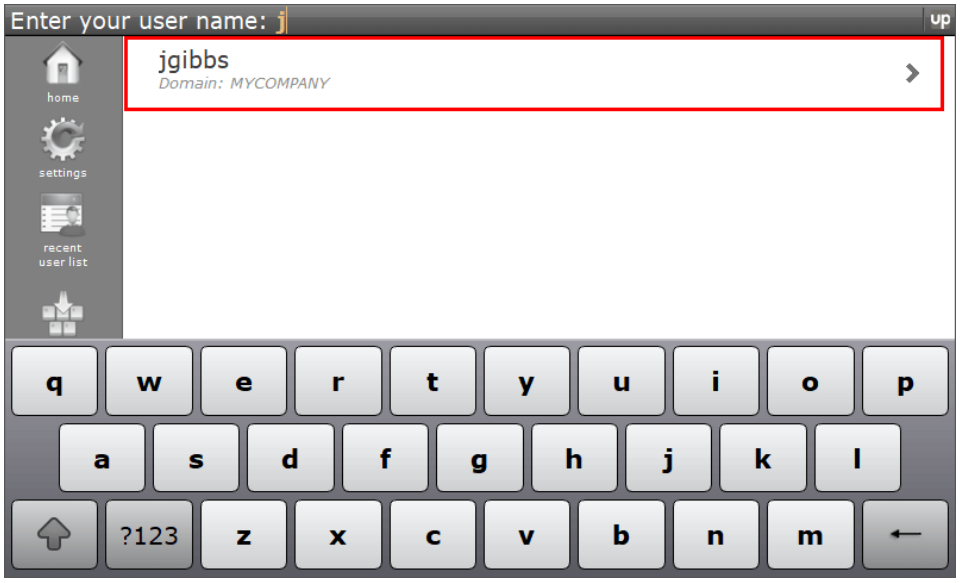


5. Enter an **Email** address, domain **UserID** and **User Domain** and then click **OK**.

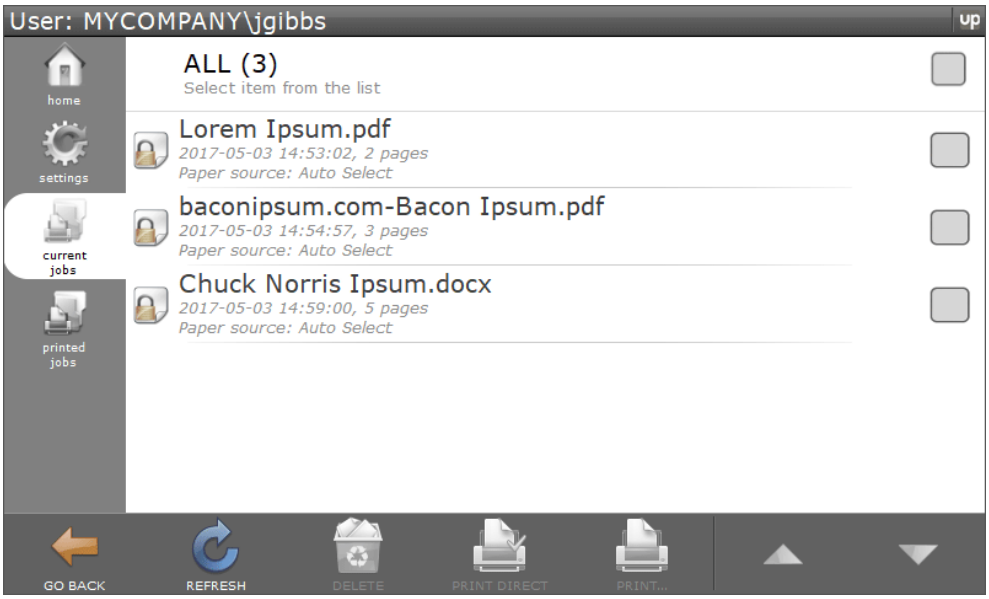


6. Repeat steps 4 and 5 to add other e-mail addresses for this user. Alternatively, a list of e-mail addresses and domain user names can also be imported into SecurePrint, refer to "Importing a List of E-mail Addresses and User Names" on page 250.

After adding all of the user's e-mail addresses, at the vPad device, the user only needs to enter and then tap their domain user name.



All of the user's print jobs sent from various e-mail addresses will appear and are available for release under their domain user name.



Importing a List of E-mail Addresses and User Names

An alternative to entering each email address one by one, is to import a list of e-mail addresses. To do this, an e-mail address and domain user name list must first be created. The list must have an e-mail address, user name, and domain name which can either be delimited with commas, spaces, semicolons or tabs and be saved either as a text (.txt) file or comma delimited (.csv) file. The domain name can be omitted, if all of your users belong to the same domain.

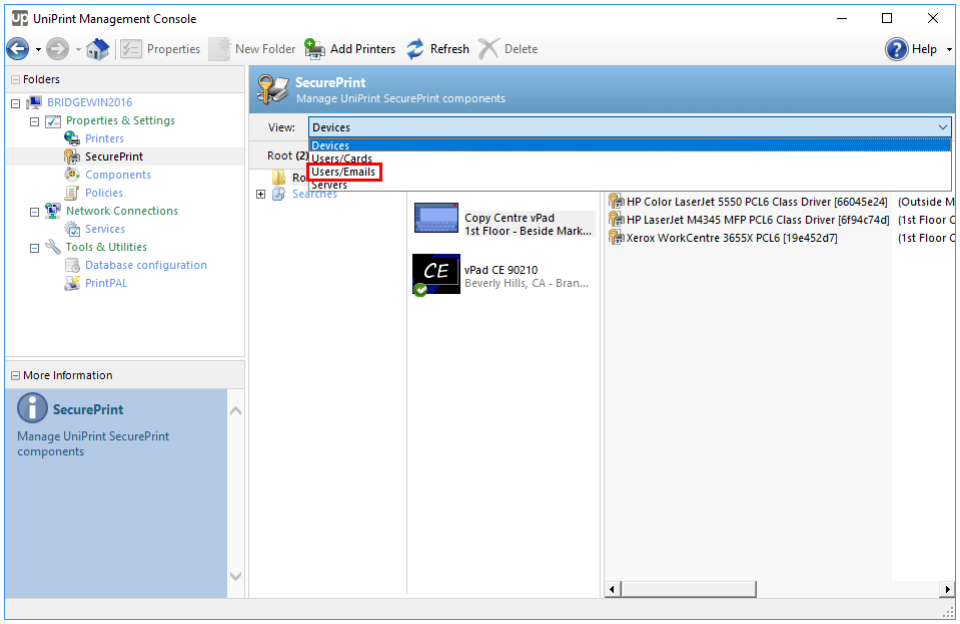
NOTE: When creating the list of e-mail addresses and user names, ensure that spaces are not added after commas or semicolons, when using commas or semicolons as delimiters.

After creating a list of e-mail addresses and user names, do the following to import it into SecurePrint:

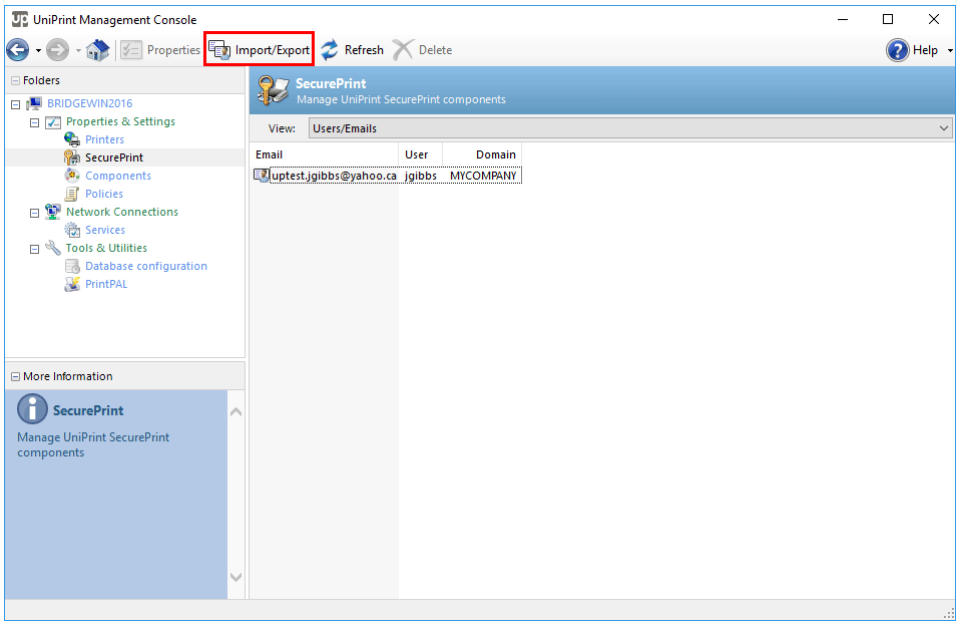
1. On the SecurePrint server (UniPrint Bridge), open the **UniPrint Management Console**.

2. Under **Properties & Settings**, click **SecurePrint**.

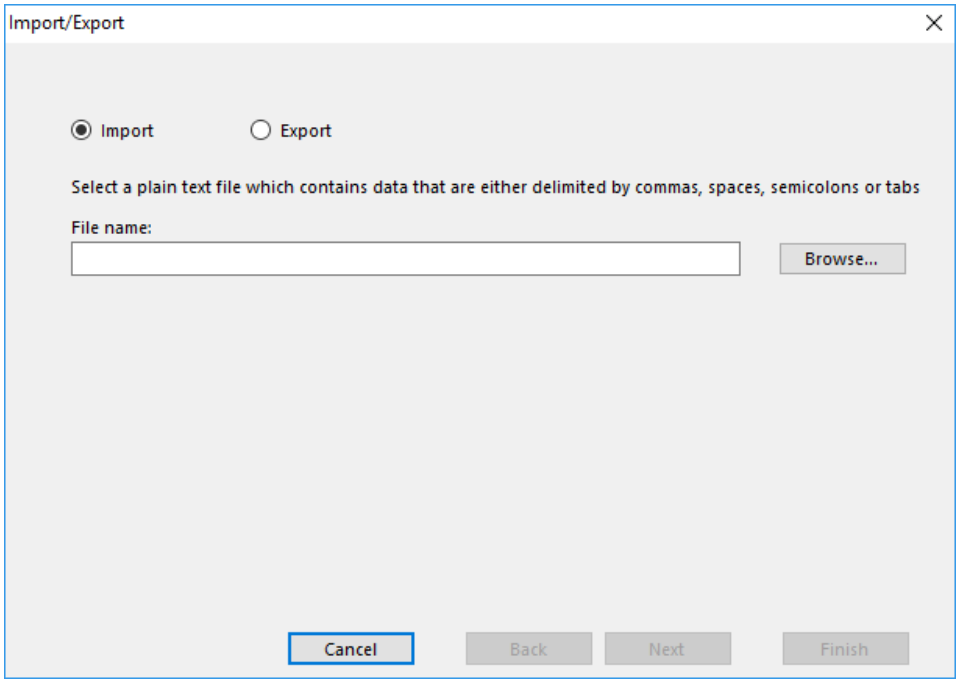
3. In the **View** menu, click **Users/Emails**.



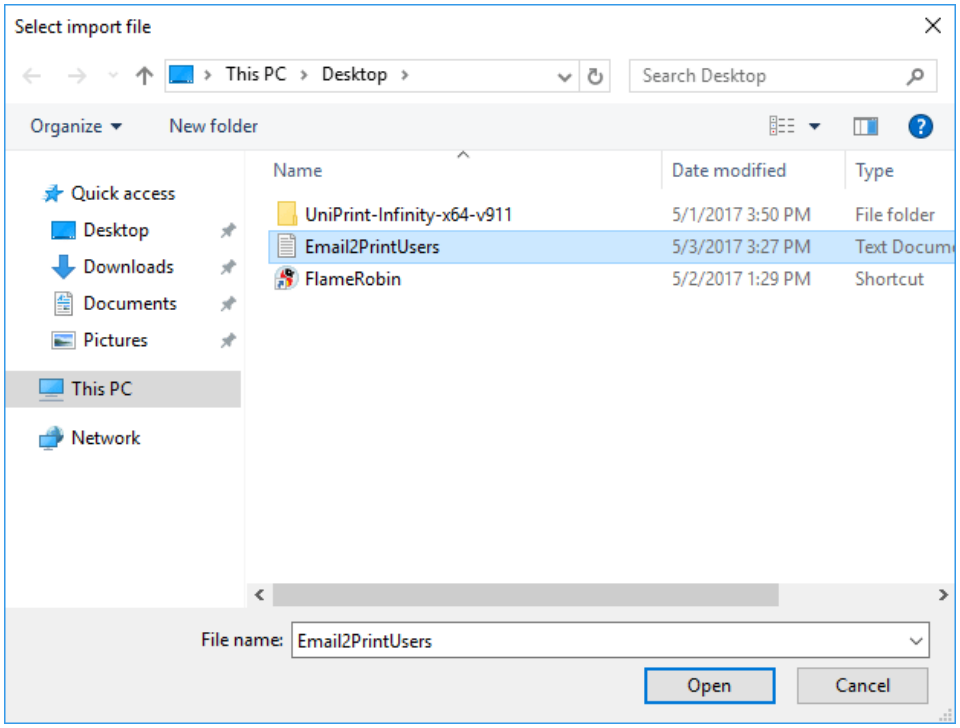
4. Click **Import/Export**.



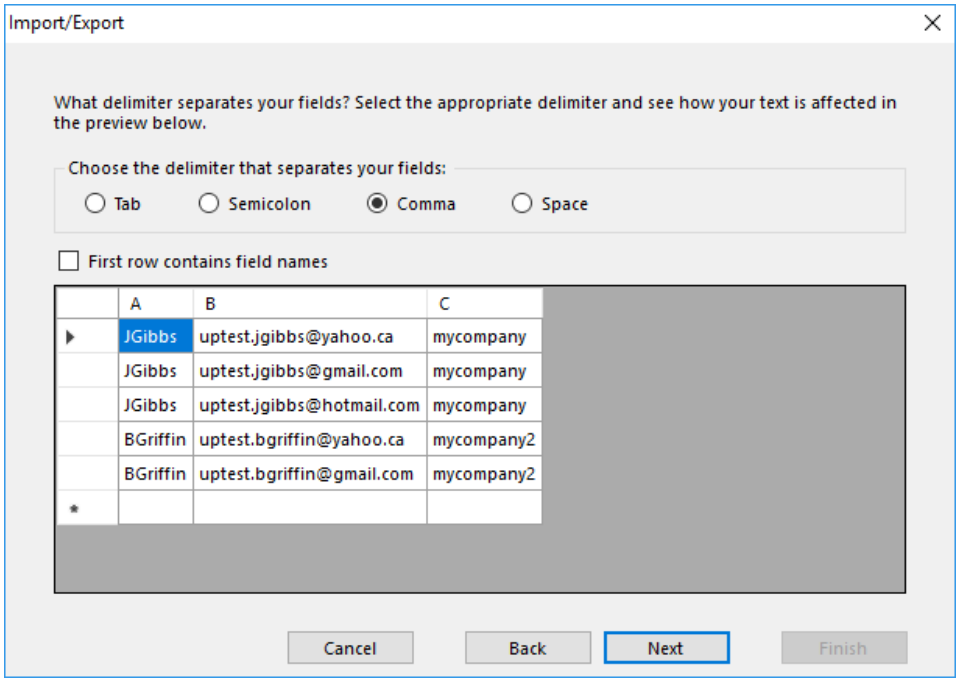
5. Ensure that **Import** is selected and then click **Browse**.



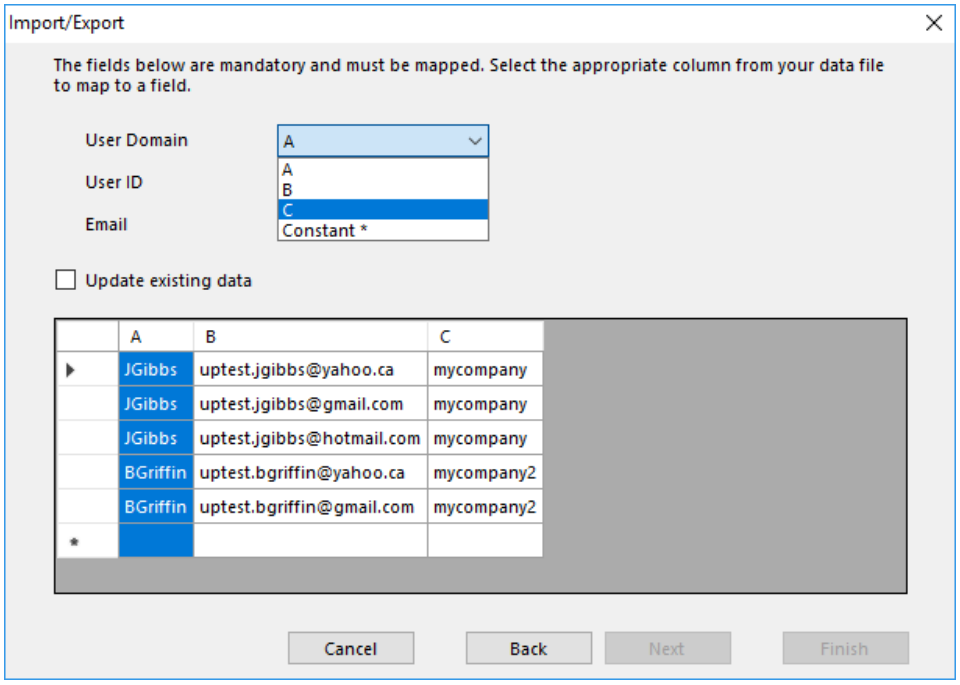
6. Click to select the file to import and then click **Open**.



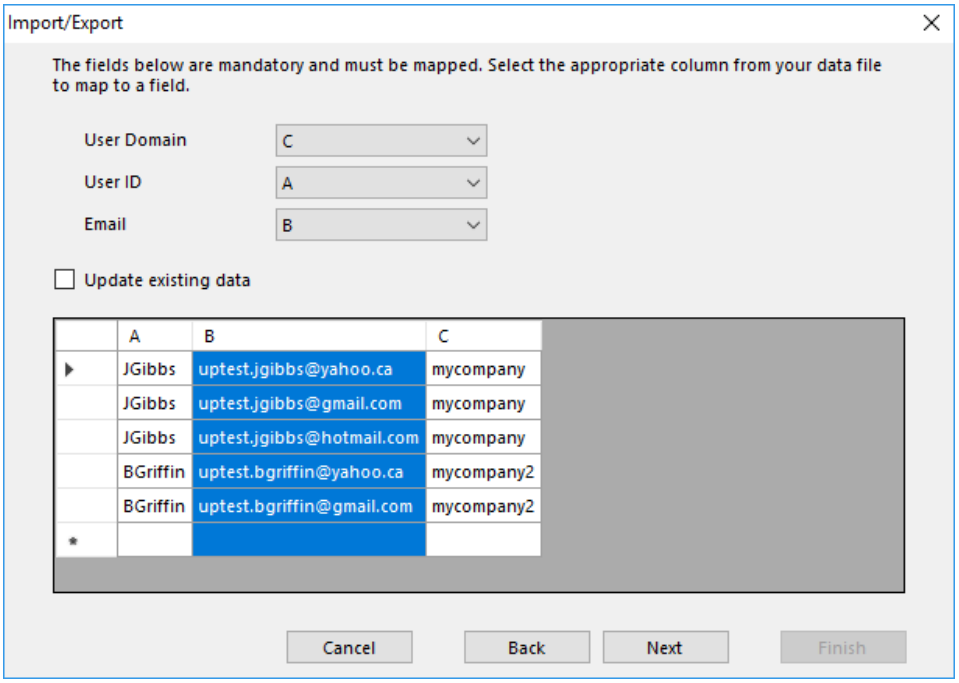
7. Select the delimiter used and then click **Next**.



8. Beside **User Domain**, click to select appropriate column. If all users are in the same domain, click **Constant** and then enter the domain name.

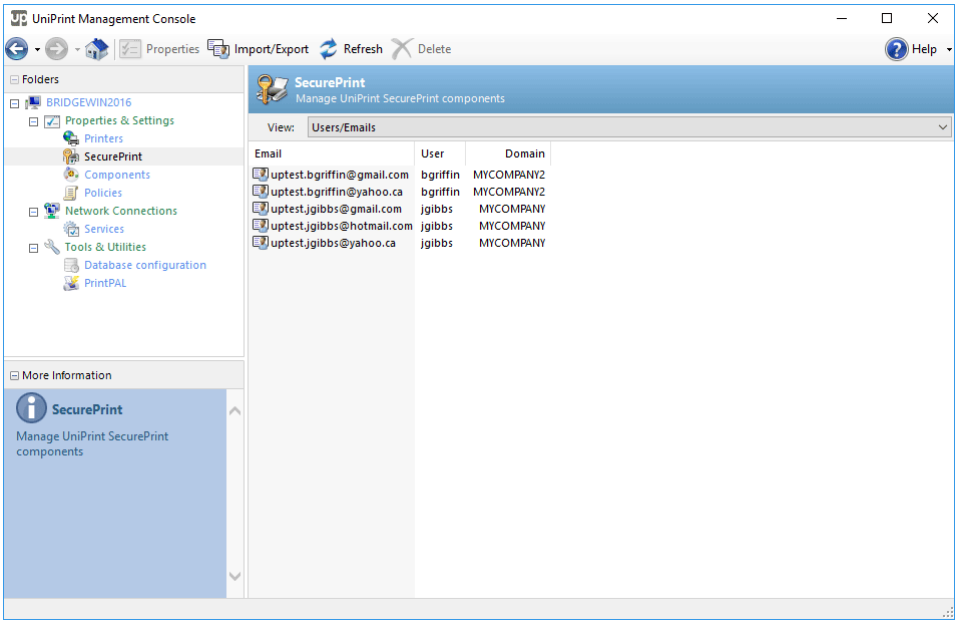


9. Select the appropriate columns for **User ID** and **Email** address and then click **Next**.



10. Click **Finish**.

All of the users and their e-mail addresses will appear in the list.

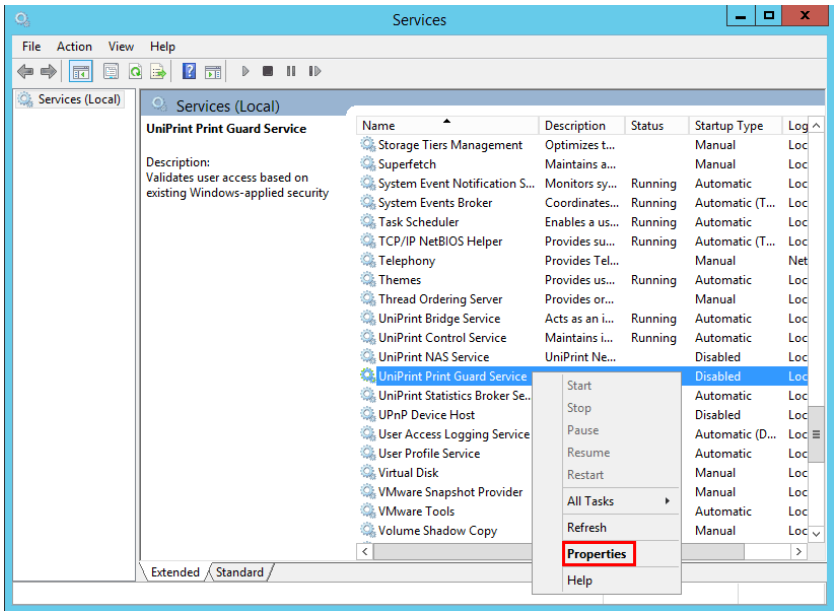


Limiting The Number Of Printers Viewed On The vPad

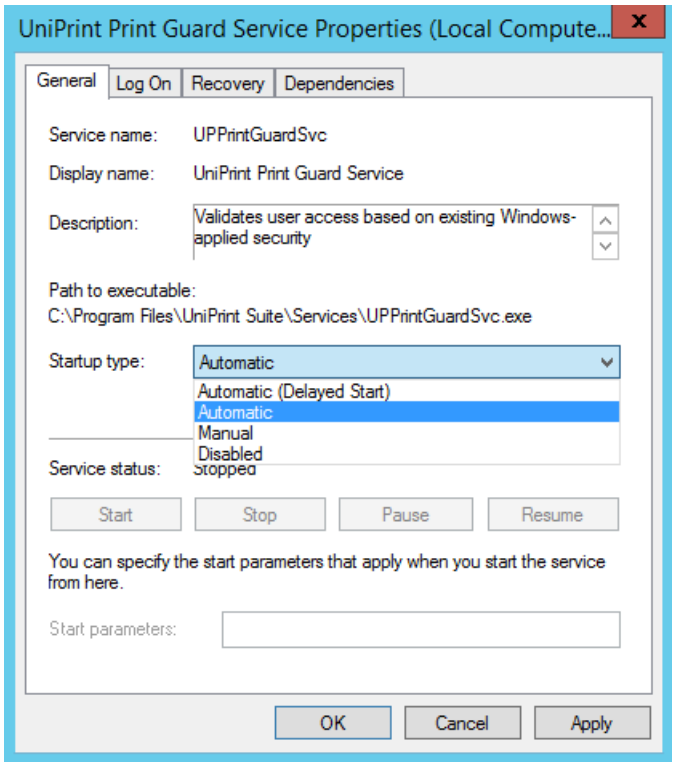
After a user prints and goes to the vPad, they could be presented with an ominous list of printers that are available in your domain. To limit the number of printers that are presented to the user on the vPad, do the following:

1. On the SecurePrint Server (UniPrint Bridge), click **Start**, click **Administrative Tools** and then double-click **Services**.

2. Right-click **UniPrint Print Guard Service** and then select **Properties**.



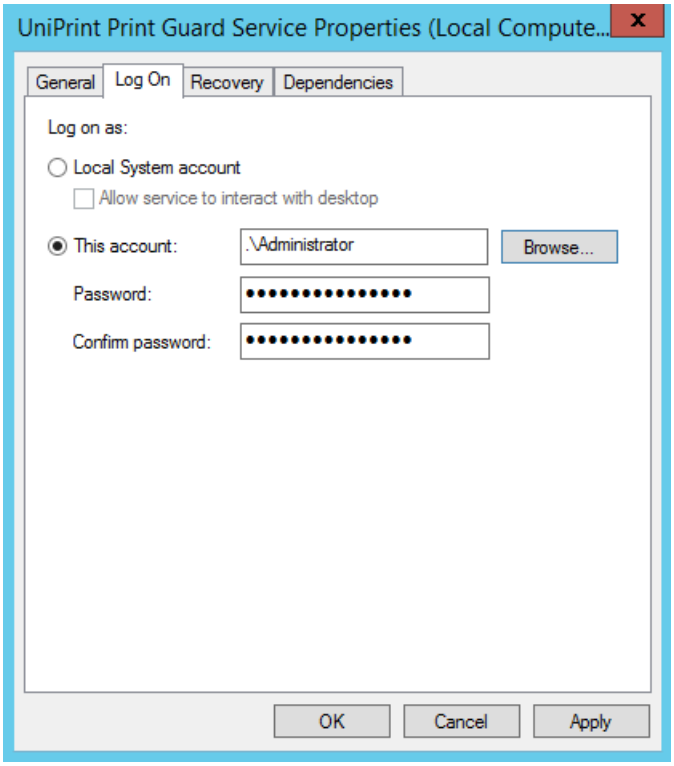
3. From the **Startup type** list, select **Automatic**.



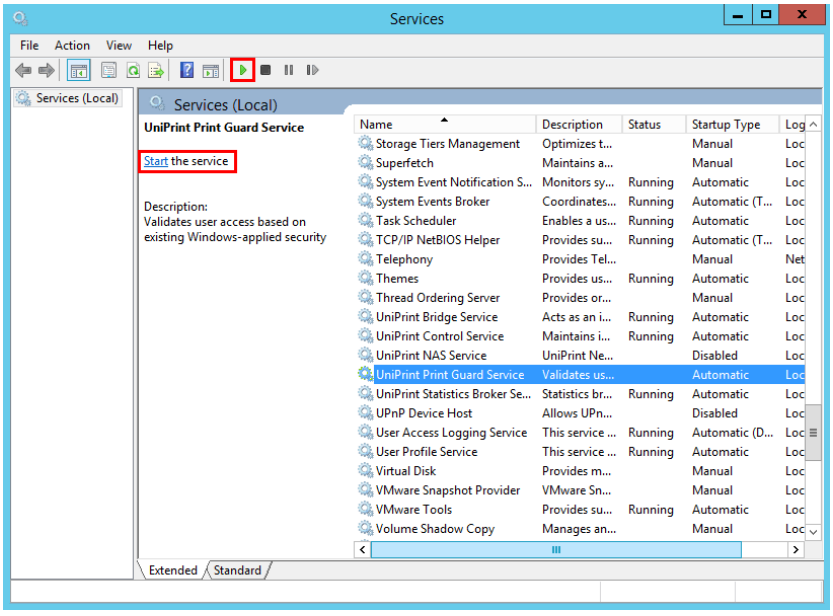
4. Click the **Log On** tab.

5. Select **This account** and enter either domain administrator or domain user credentials and then click **OK**. ***Note****: The Print Guard*

Service needs to run as either a domain administrator or domain user with local administrator rights on the SecurePrint Server (UniPrint Bridge).

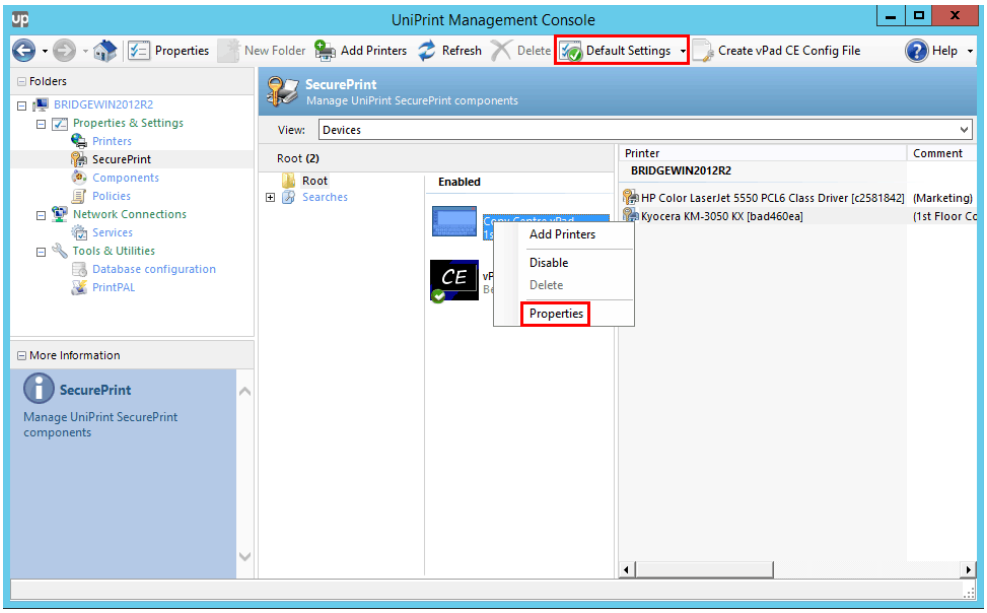


6. Start **UniPrint Print Guard Service**.



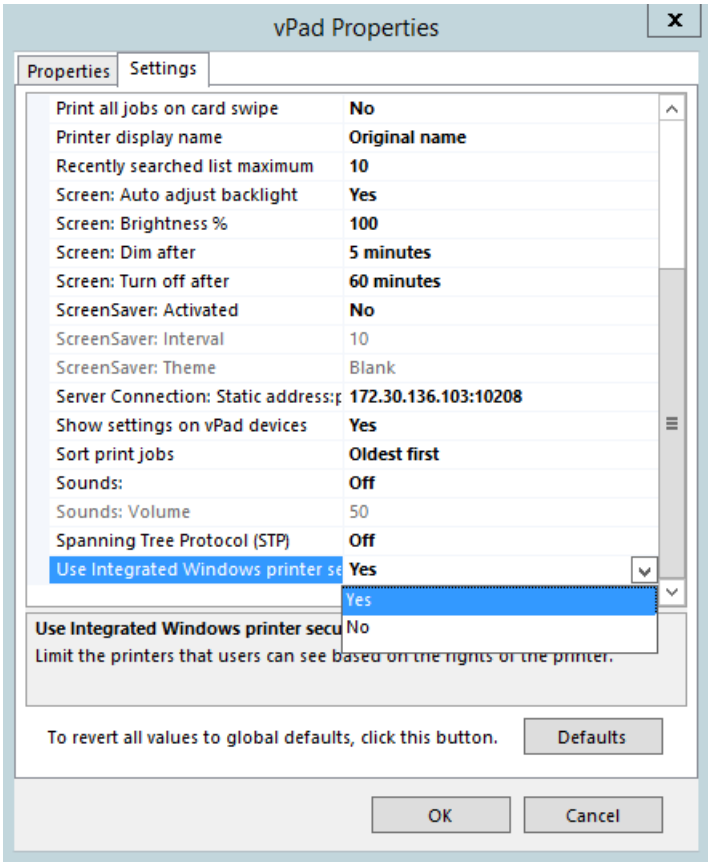
7. Open the **UniPrint Management Console** and then click **SecurePrint**.

8. Either right-click a vPad to change an individual device or click **Default Settings** to change global vPad properties.



9. Click the **Settings** tab.

10. Set **Use Integrated Windows printer security** to **Yes**.



11. Click **OK**.

12. Deny printer access by modifying the Access Control List of Gateway printer(s) located on the UniPrint Bridge, *not the print server*.

Enabling Users To Print All Jobs With A Single Swipe Of Their Card

If a default printer is set for the vPad, users can send all of their active print jobs to the default printer by swiping their cards only. This option bypasses the requirement for users to authenticate by both swiping their cards and entering their password.

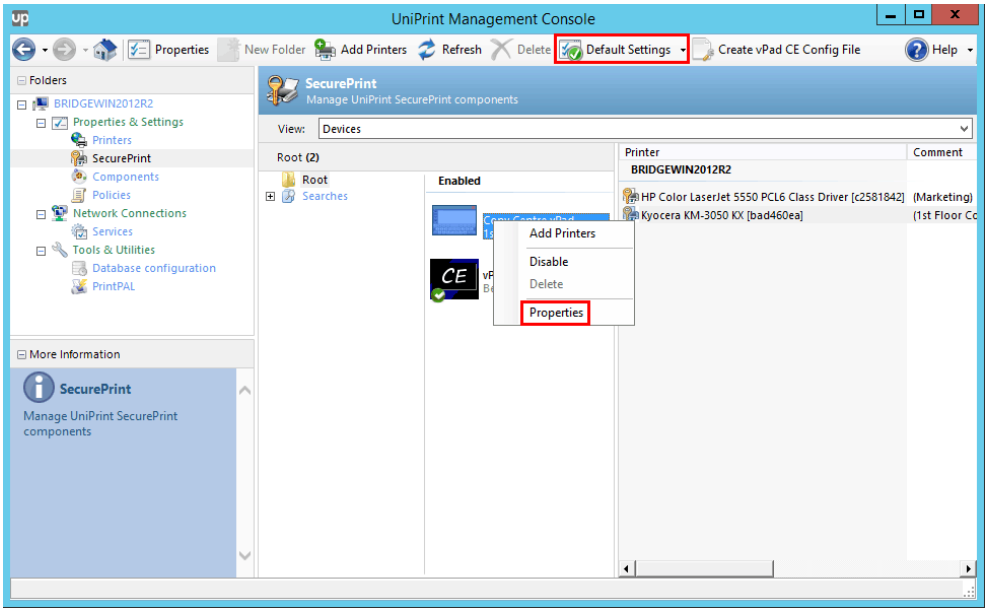
NOTE: If the user prints to multiple password-protected Gateway printer queues then the user will be prompted to select a printer on the vPad.

To enable this option, do the following:

1. On the **UniPrint Bridge**, open the **UniPrint Management Console**.

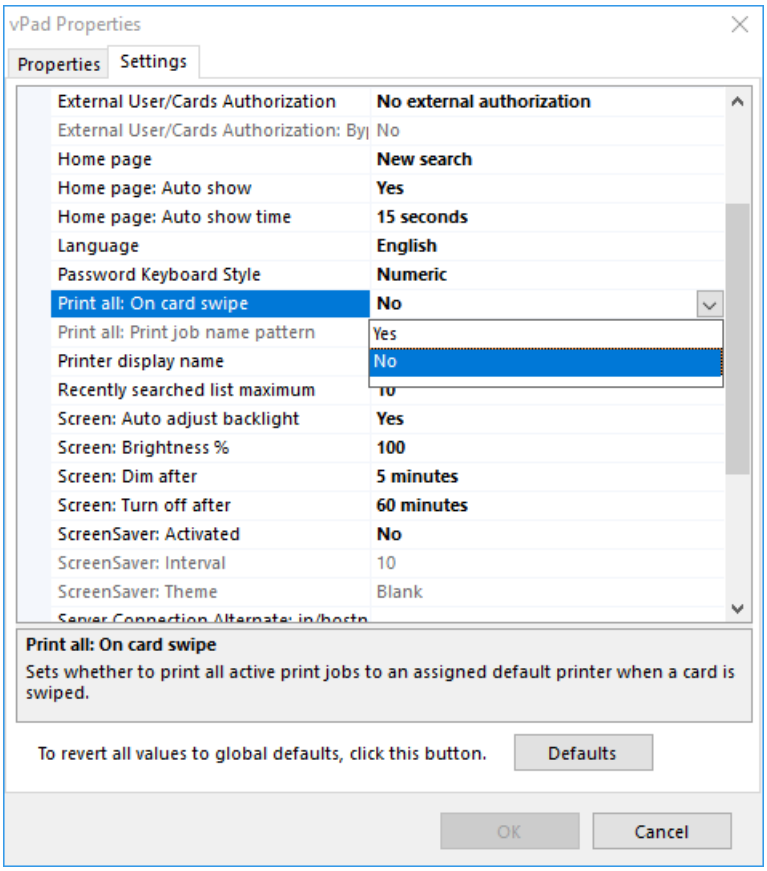
2. Under **Properties & Settings**, click **SecurePrint**.

3. To enable this option for all vPads, click **Default Settings**. To enable this option for a specific vPad, right-click the vPad and then select **Properties**.



4. Click the **Settings** tab.

5. Set **Print all: On card swipe** to **Yes** and then click **OK**.



vPad Print Job Filtering

When **Print all: On card swipe** is set to **Yes**, the user is unable to select individual print jobs. Once the user taps their RFID/HID card at the vPad, all print jobs will automatically print to the default printer that is associated with that vPad. However, by using vPad Print Job Filtering, print jobs can be filtered such that only certain print jobs that match a specified filter will print. vPad Print Job Filtering can be especially useful in the following scenario, since it can save paper and ink.

Example Usage Scenario

A user prints several different documents, some of which are intended for a label printer and others are intended for a regular laser printer. Since label printer supplies tend to be more expensive than typical laser printers, the company decided to associate one vPad to one label printer. The user wants to print the labels first and goes to the vPad and taps their RFID/HID card. As a result, all the labels print, but so do the other print jobs that were intended to print at a typical laser printer. The solution is to use vPad Print Job Filtering and specify that if a word "Label" is found in the file name then print it to the label printer. The user would also need to ensure that all print jobs destined for the label printer have been renamed with the word "Label" in the file name.

To implement vPad Print Job Filtering, do the following:

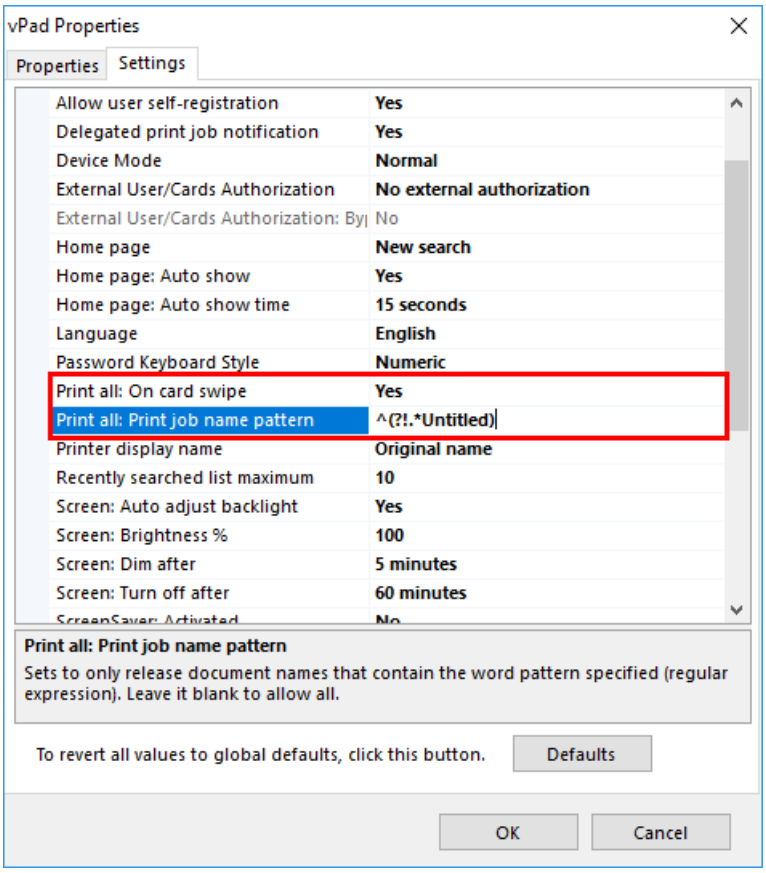
1. On the SecurePrint server (UniPrint Bridge), open the **UniPrint Management Console**.

2. Under **Properties & Settings**, click **SecurePrint**.

3. Click to select the appropriate vPad and then click **Properties**.

4. Click the **Settings** tab.

5. Beside **Print all: Print job name pattern**, enter a regular expression for UniPrint to match. For example, **`Label`** will match all print job names with the word "Label" in it. Or to exclude a string, **`^(?!.*Untitled)`** will exclude all print jobs names with the word "Untitled" in it.



6. Click **OK**.

Enabling Data Compression Between Print Server And Printer Through The vPad

In environments where the print server is located in a different geographic location from the vPad Pro/CE and the printer, the print data transmitted

from the print server to the printer will be compressed via the vPad Pro/CE device by utilizing the UniPrint Transport Port Monitor.

NOTE: Print stream compression is only functional with the vPad Pro or vPad CE device itself and the device must be enabled in the UniPrint Management Console. Print stream compression is ***not*** compatible with the vPad Touch or the SecurePrint Emulator. The SecurePrint Server component must still be installed even if only Print Stream Compression is being deployed without the UniPrint VPQ. Print stream compression supports up to 5 concurrent print jobs at a time.

NOTE: Due to design changes in Windows 8.1 and Windows Server 2012 R2, the UniPrint Transport Port can only be checked using Type 3 printer drivers. Print Stream Compression is not compatible with Type 4 printer drivers. For more information, consult http://social.technet.microsoft.com/Forums/windowsserver/en-US/09eaabcb-7f62-44e9-8db7-998b5d35f9bc/cant-change-printer-port-on-windows-81-and-server-2012-r2?forum=winserver8gen

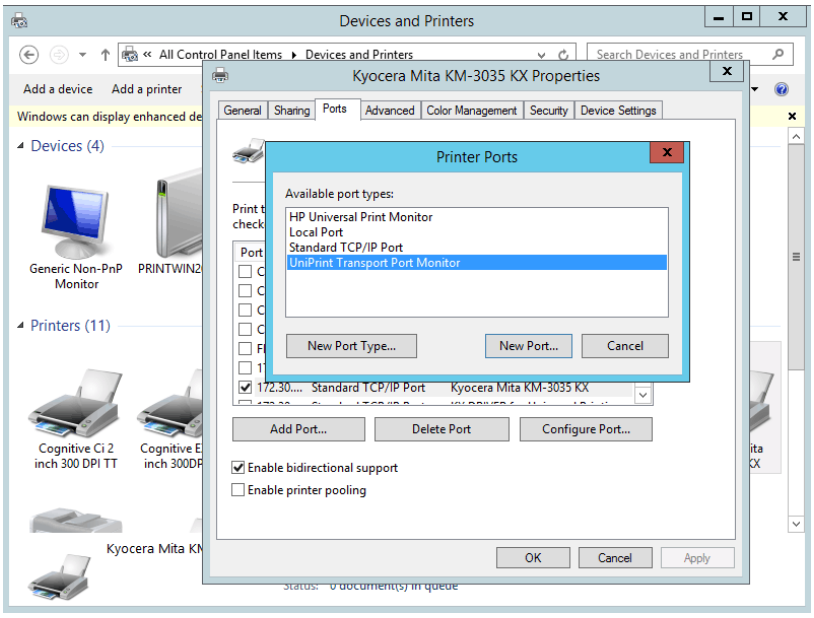
To enable this feature, do the following:

1. On the **UniPrint Print Server**, open the **Control Panel** and then double-click **Devices and Printers**.

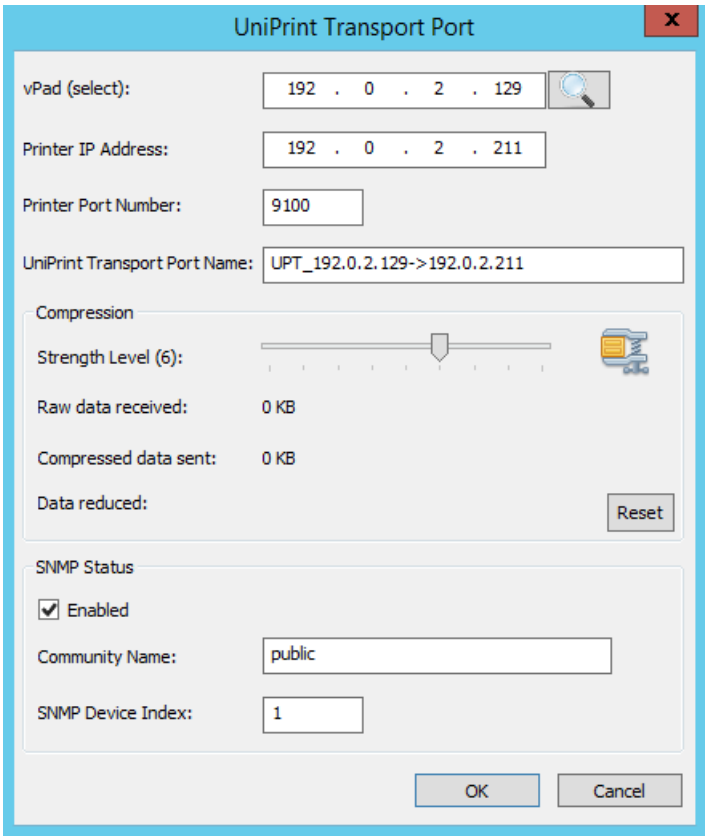
2. Right-click a printer that is associated with the vPad or vPad CE and then select **Printer properties**. ***Note****: To add a port, you must either be logged in as the built-in "Administrator" or you must have UAC disabled.*

3. Click the **Ports** tab and then click **Add Port**.

4. Click to select **UniPrint Transport Port Monitor** and then click **New Port**.



5. Enter the **vPad IP Address** and the **Printer IP Address**. Adjust the compression strength to the desired level and then click **OK**.



6. Click **Close** and then click **Apply**.

7. Click **OK** again.

Viewing Compression Statistics

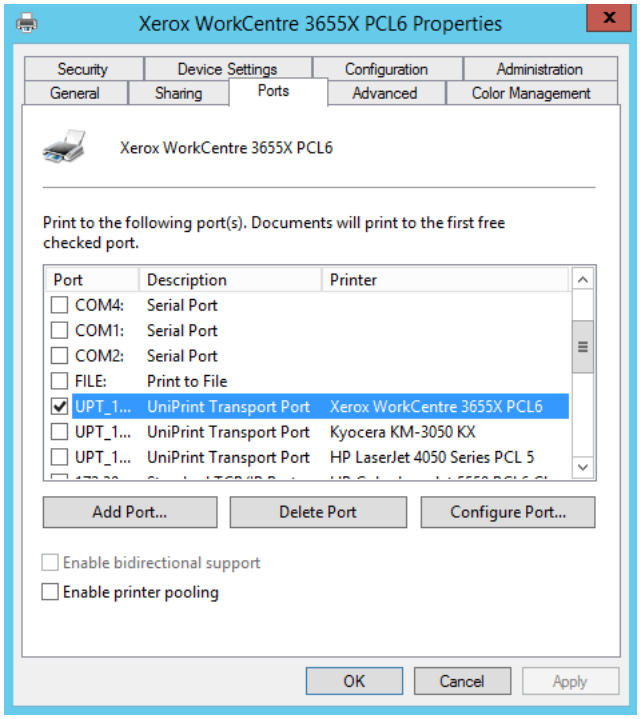
After the UniPrint Transport Port Monitor has been configured, all print jobs sent that printer will be compressed at the print server and then decompressed at the vPad or vPad CE.

To check the amount of compression and data that is being processed by the UniPrint Transport Port Monitor, do the following:

1. On the **UniPrint Print Server**, open the **Control Panel** and then double-click **Devices and Printers**.

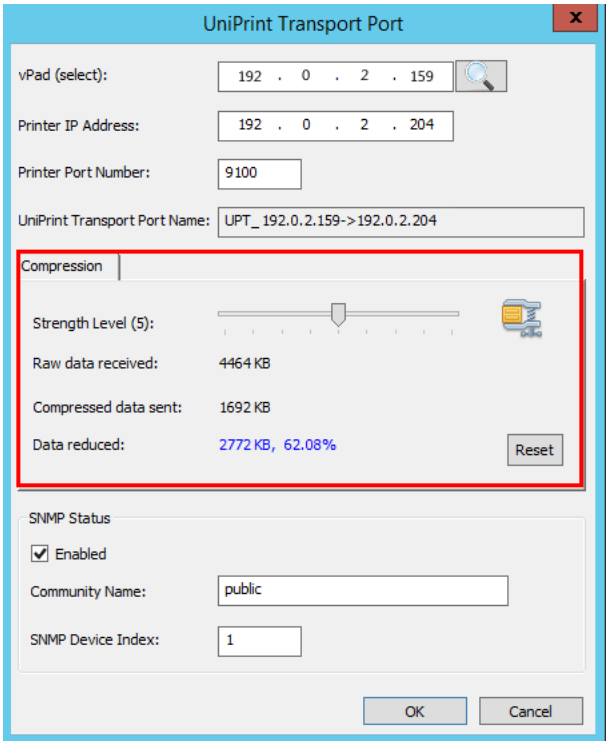
2. Right-click a printer that is associated with the vPad or vPad CE and then select **Printer properties**. ***Note****: To view port information, you must either be logged in as the built-in "Administrator" or you must have UAC disabled.*

3. Click the **Ports** tab and then click **Configure Port**.



4. The amount of compression and the amount of raw data processed is reported as well as the level of compression. To increase or decrease

the amount of compression, slide the slider accordingly. To reset the compression statistics back to zero, click **Reset**.



Troubleshooting Print Stream Compression

If issues arise from print stream compression then enable logging of the UniPrint Transport Port Monitor component and then contact UniPrint Support.

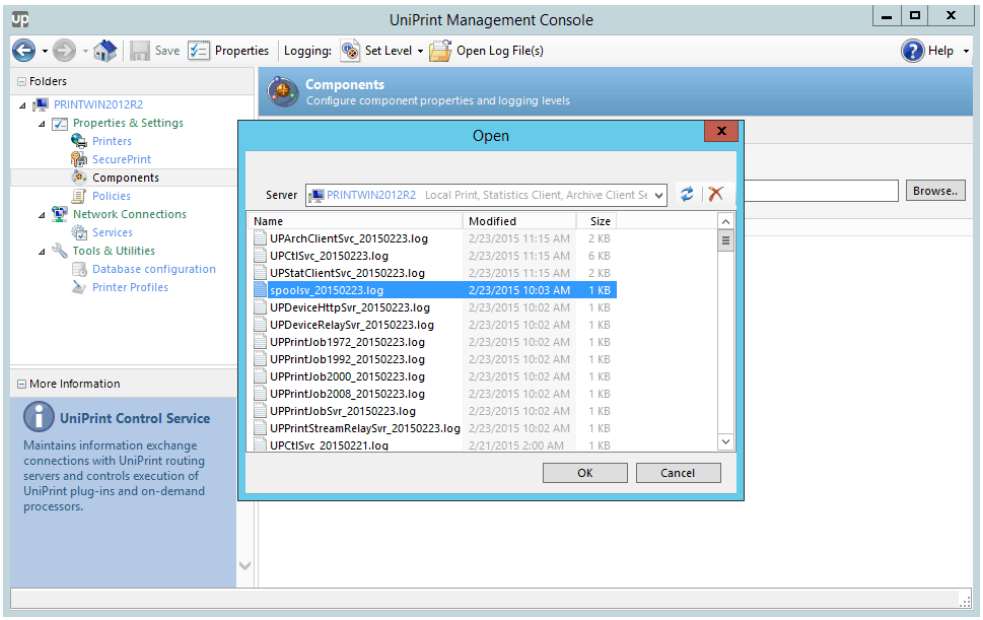
To enable logging, do the following:

1. On the **UniPrint Print Server**, open the registry editor.

2. Under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Monitors\UniPrint Transport Port Monitor create a new DWORD value named `LogLevel`.

3. Assign the **LogLevel** a value of `3` (high) to log and capture issues and errors.

The log can be viewed through the UniPrint Management Console. Click **Components** and then click **Open Log File(s)**. Select **spoolsv.log**.



Setting up Imprivata OneSign for SecurePrint Authentication

Imprivata authentication and password management can be easily integrated into UniPrint Infinity's SecurePrint. This enables the user to use their Imprivata proximity card to unlock and authenticate on the UniPrint vPad before releasing their SecurePrint print jobs.

NOTE: An additional licensing fee is required for Imprivata integration. Contact your UniPrint Territory Manager for more information.

Installing the Imprivata Gateway Component

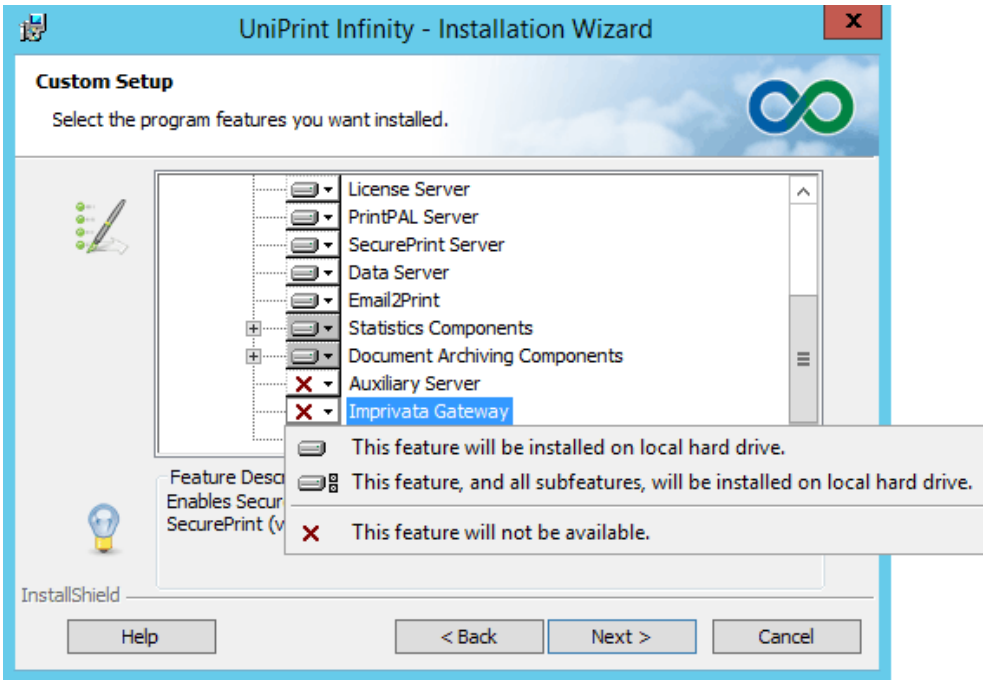
The following instructions assumes that UniPrint Infinity has already been installed using the Print Server scenario. Imprivata Gateway can also be installed during a fresh installation of UniPrint Infinity. The Imprivata Gateway component is installed on the same machine as the SecurePrint Server.

1. On the UniPrint Bridge (SecurePrint Server), run the installation program, **UniPrint91_*.exe** as an administrator.

2. In the **UniPrint Infinity Maintenance** dialog box, click **Next**.

3. In the **Program Maintenance** dialog box, ensure the **Modify** is selected and then click **Next**.

4. In the **Custom Setup** dialog box, beside **Imprivata Gateway**, click and then select **This feature will be installed on local hard drive**. Click **Next**.



5. In the **Ready to Modify the Program** dialog box, click **Install**.

6. Click **Finish** to complete the installation.

Integrating UniPrint Infinity on the Imprivata OneSign Server

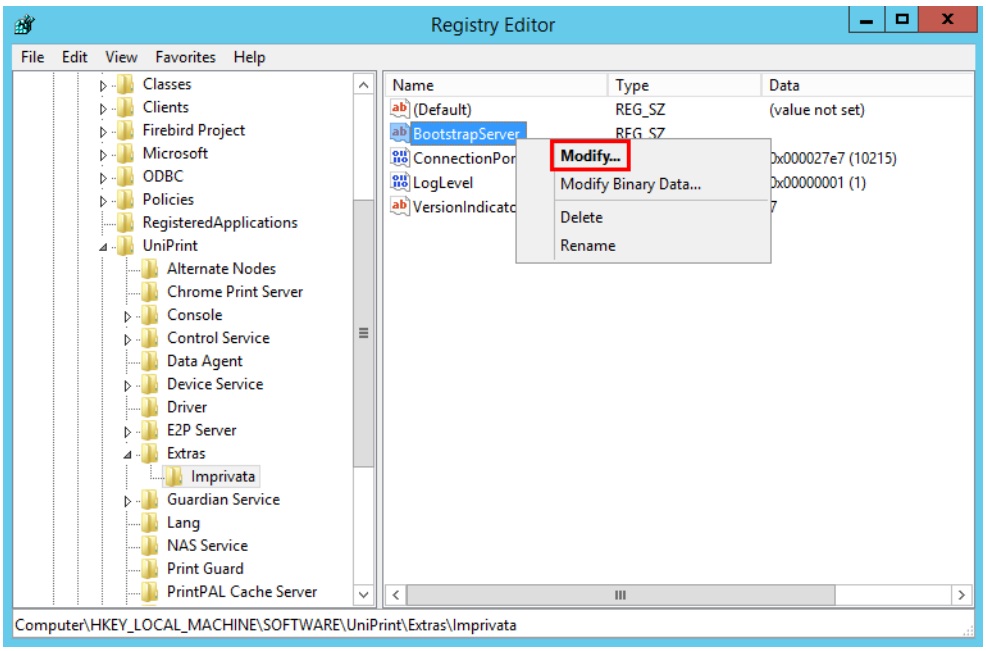
Since Imprivata OneSign is deployed differently depending on the organization, the actual steps may vary depending on your OneSign deployment. Contact support@uniprint.net for assistance in integrating UniPrint Infinity on the OneSign server.

Configuring SecurePrint to Recognize Imprivata OneSign

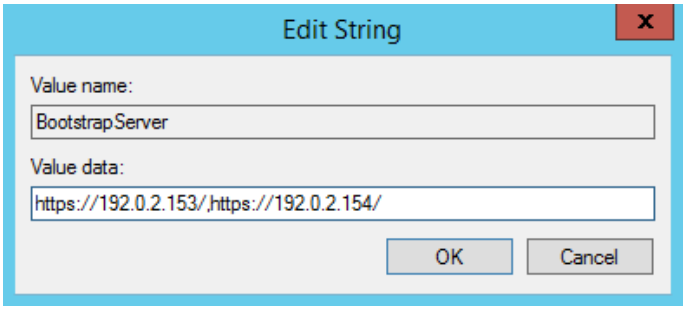
After installing the Imprivata Gateway component on the SecurePrint Server and integrating UniPrint Infinity on a Imprivata OneSign server, SecurePrint needs to be configured to recognize Imprivata OneSign as the preferred form of authentication.

1. On the UniPrint Bridge (SecurePrint Server), open the **Registry Editor**.

2. Under the registry key, **HKEY_LOCAL_MACHINE\Software\UniPrint\Extras\Imprivata**, right-click **BootstrapServer** and then select **Modify**.



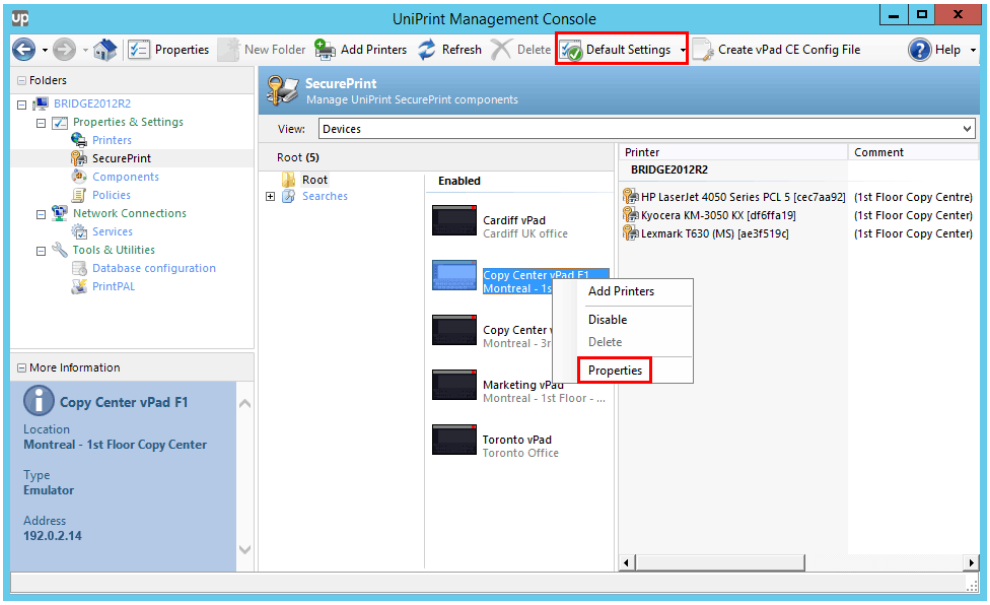
3. Under **Value data**, enter the URL of the Imprivata OneSign server using either an IP address or host name and then click **OK**. ***Note**: IP addresses must be entered in the format of* **`https://[IP address]/`**. *Multiple IP addresses and host names must be separated by a comma.*



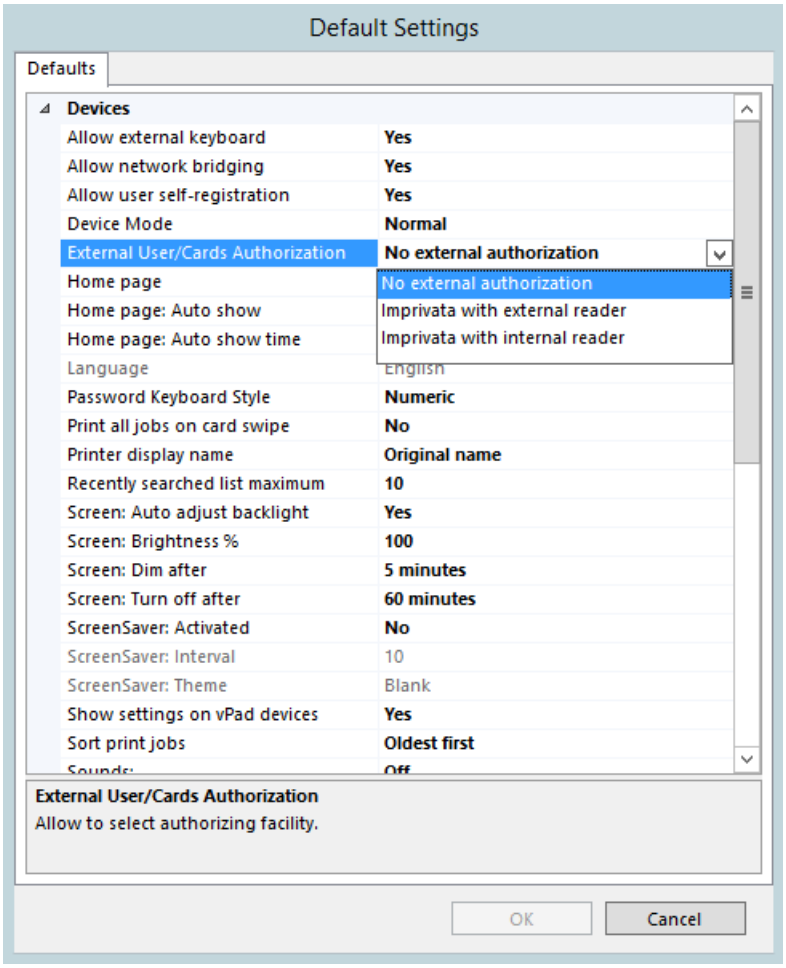
4. Open the **UniPrint Management Console**.

5. Under **Properties & Settings**, click **SecurePrint**.

6. To enable Imprivata OneSign globally for all vPad Pro devices, click **Default Settings**. To enable Imprivata for only one vPad Pro, right-click the vPad and then click **Properties**.



7. From the **External User/Cards Authorization** list, select either **Imprivata with external reader** or I**mprivata with internal reader** depending on the type of card readers used. Click **OK**.



Configuring The UniPrint vPad Device

The vPad is a device that was designed in conjunction with SecurePrint and the VPQ (virtual print queue). The vPad securely controls access to stored print jobs and is printer model independent. Since more than one printer can be associated with a vPad device, only one vPad is required for a group of printers located in close proximity of each other.

Configuring the process of secure pull-printing is done on the UniPrint Management Console, however the device itself can be configured to reduce memory consumption and adjust screen brightness for example.

The following tasks can only be done if the administrator has enabled **Show settings on vPad devices** on the SecurePrint Server (UniPrint Bridge).

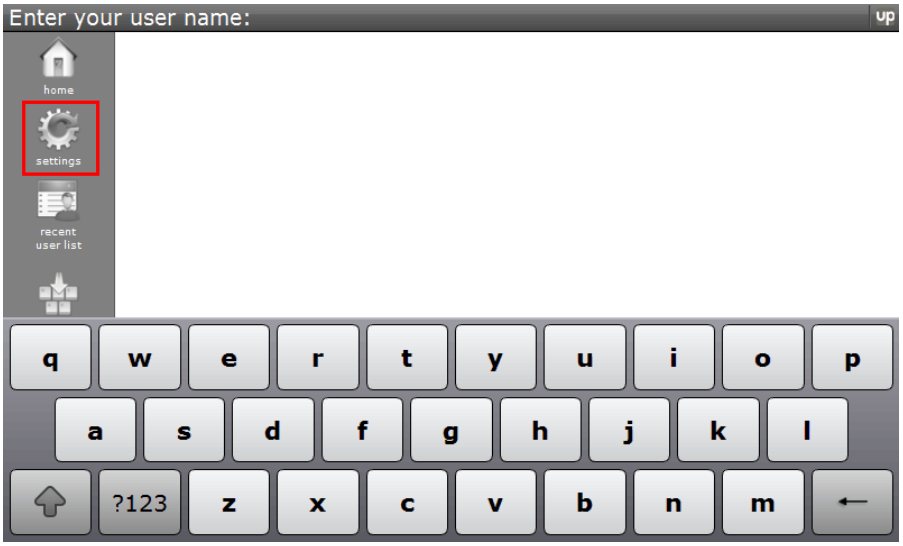
Some features only apply to the vPad Pro and not to the SecurePrint emulator, vPad Touch or vPad CE.

Adjusting Screen Brightness and Backlighting

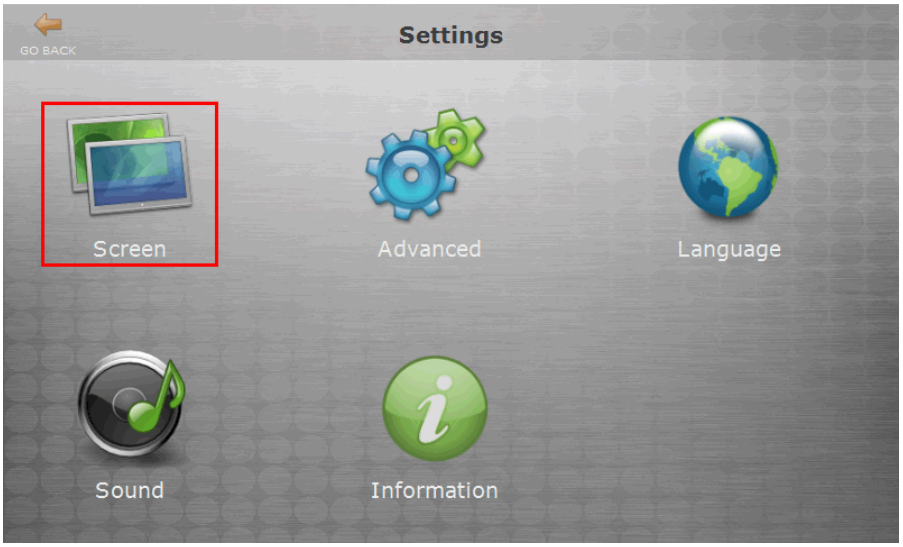
The following feature only applies to the vPad Stand and Pro and not to the SecurePrint emulator or vPad Touch. To adjust the screen brightness and backlighting for the SecurePrint emulator and vPad Touch, use the Control Panel in Windows.

To adjust the screen brightness and backlighting, do the following:

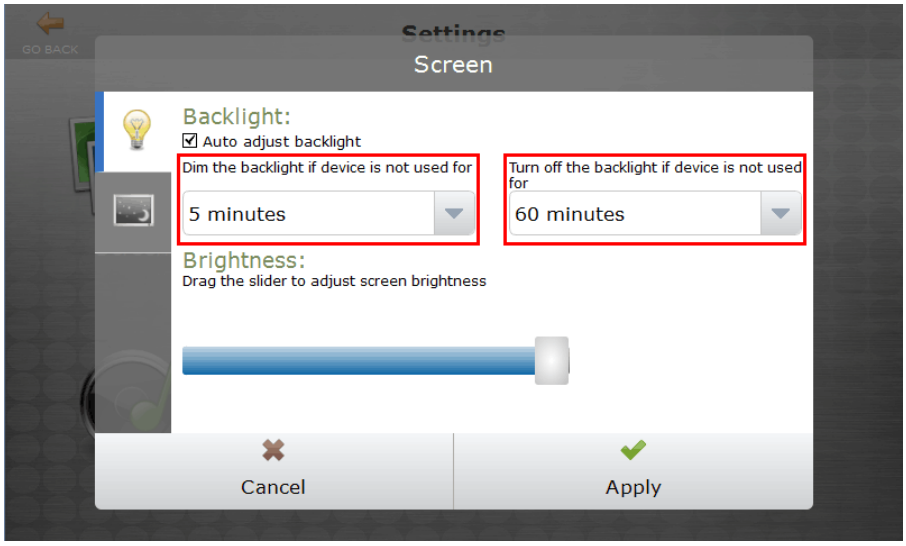
1. In the Home page, tap **Settings**.



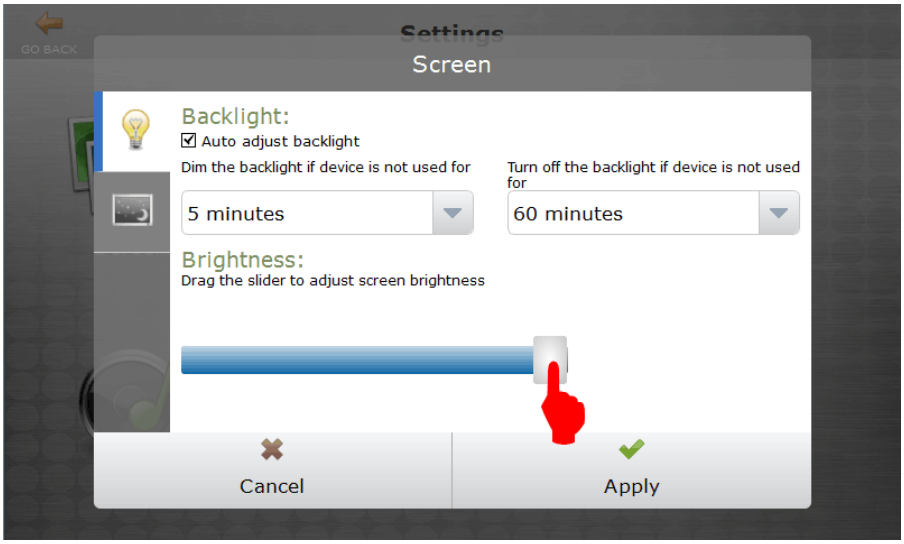
2. Tap **Screen**.



3. Adjust screen idle time when you would like the backlight to dim and turn off by selecting the appropriate time from the lists.



4. Adjust the screen brightness by dragging the slider to appropriate level.



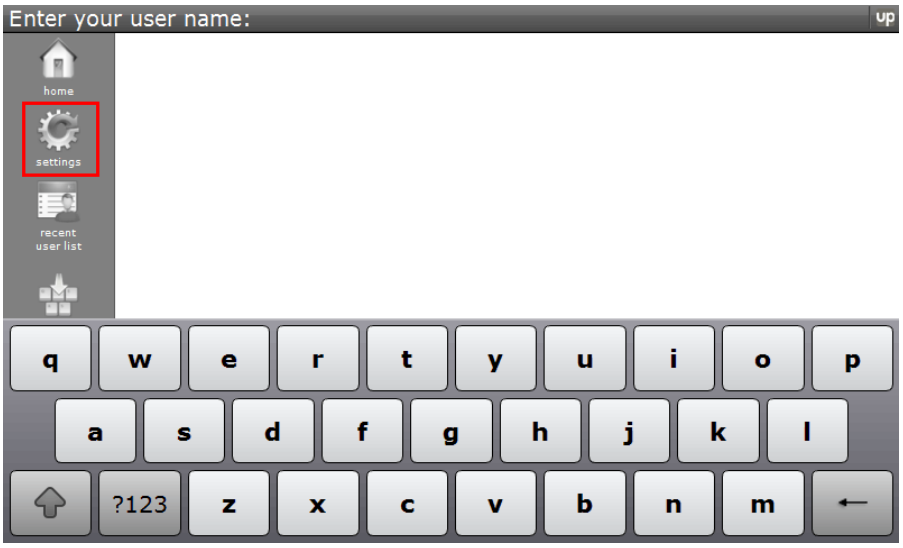
5. Tap **Apply**.

Setting Up A Screensaver

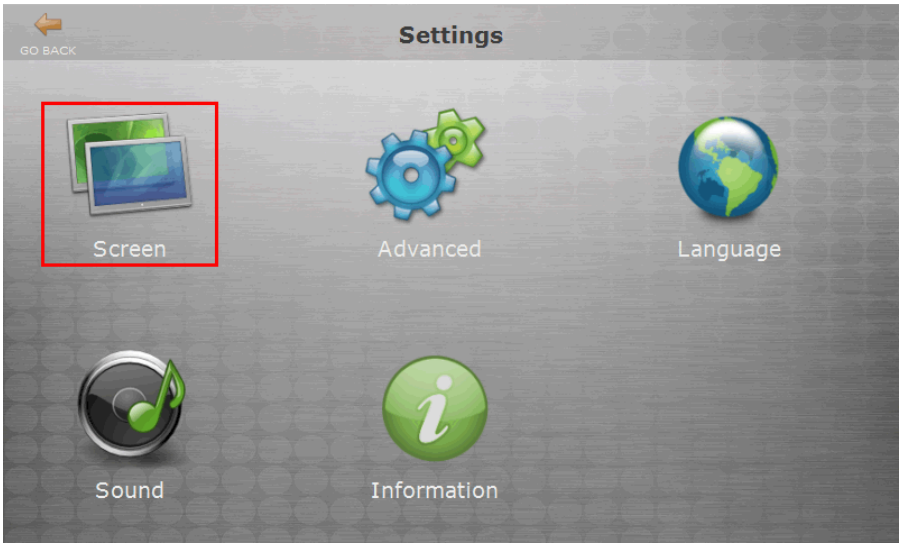
The following feature only applies to the vPad Standard, and Pro only. It does not apply to the SecurePrint emulator or vPad Touch. To adjust the screen saver for the SecurePrint emulator and vPad Touch, use the Control Panel in Windows.

To set up a screensaver on the vPad Pro, do the following:

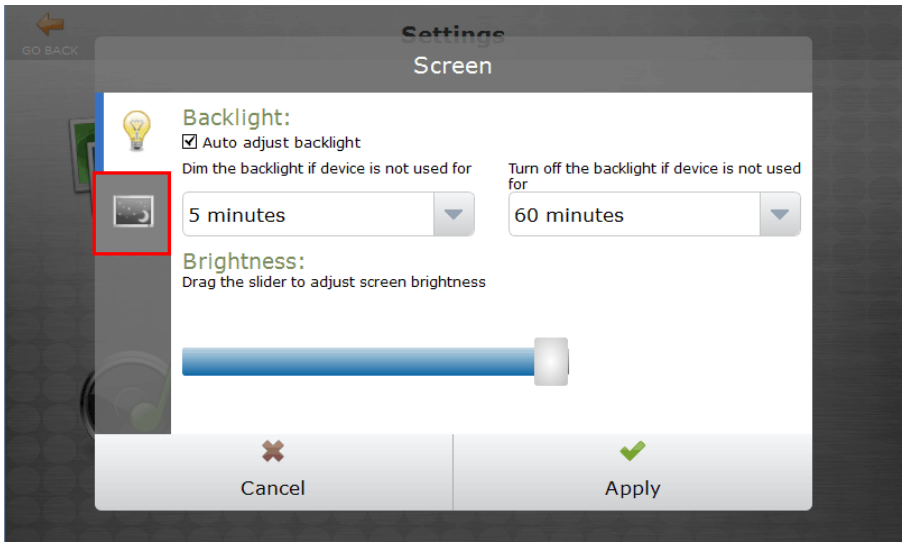
1. In the Home page, tap **Settings**.



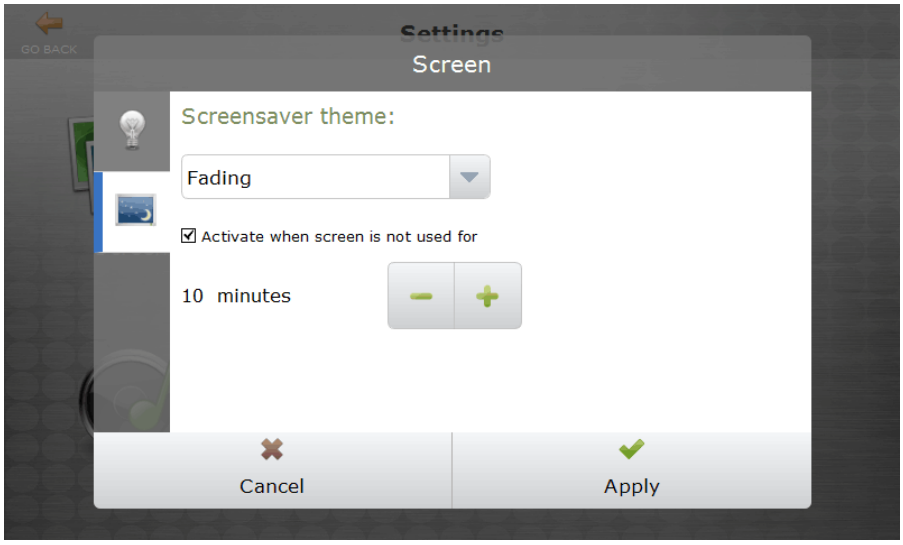
2. Tap **Screen**.



3. Tap the **Screensaver** tab.



4. Select the theme, **Fading** or **Blank** and the screen idle time required before the screensaver starts. To disable the screensaver, clear the **Activate when screen is not used for** option.



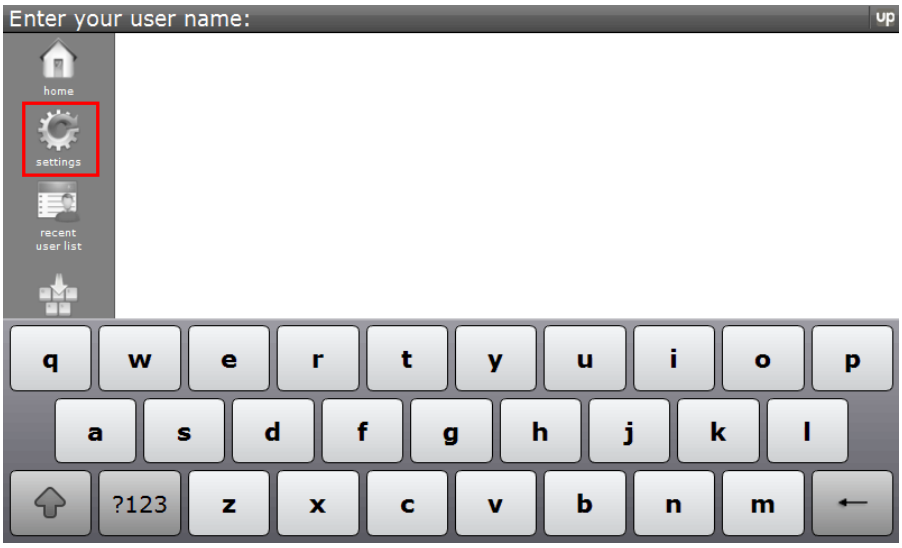
5. Tap **Apply**.

Changing the Default Home Page & Refresh To Home Page

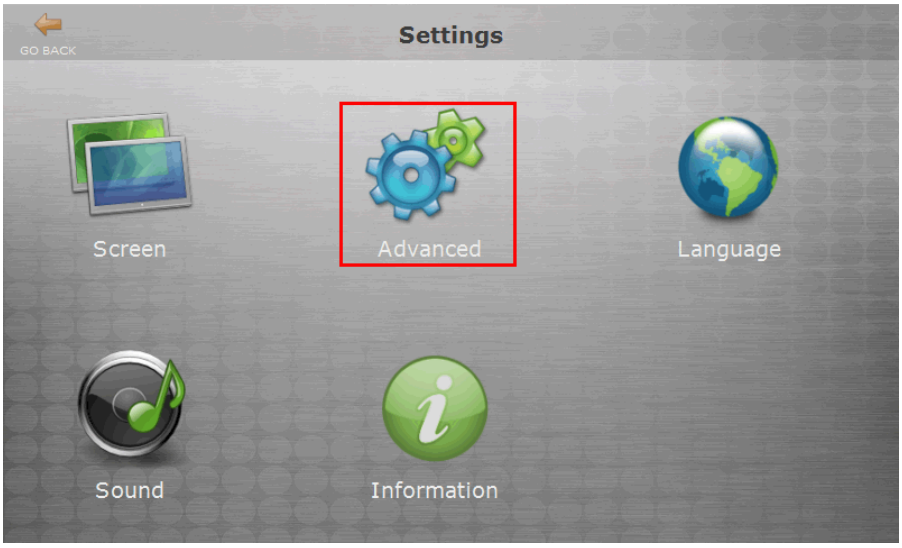
Depending on your users' preference, the home page can be set to either immediately accept their user input or to a list of recent users. The time in which the screen refreshes to the home page if left idle can also be adjusted. This feature applies to the vPad Standard, vPad Pro, vPad Touch and the SecurePrint emulator.

To change the Home page settings, do the following:

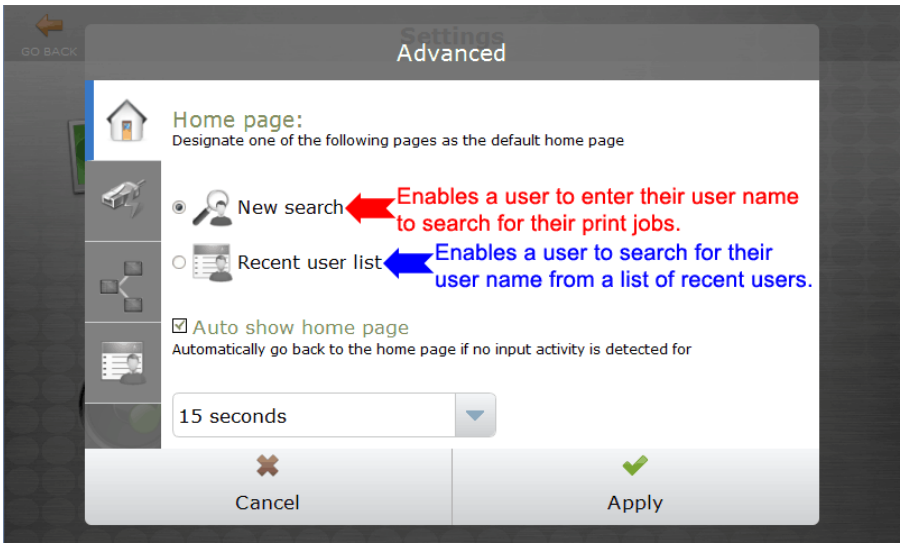
1. In the Home page, tap **Settings**.



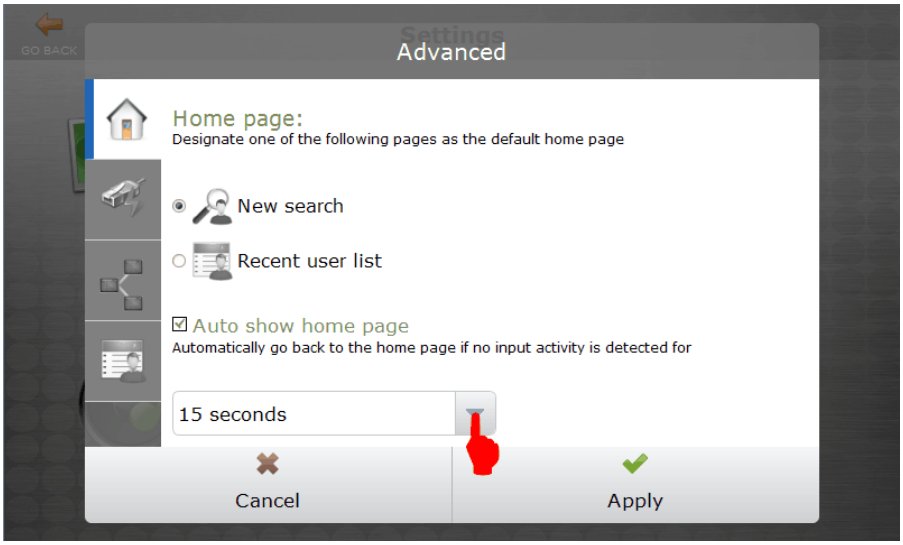
2. Tap **Advanced**.



3. Tap either **New search** or **Recent user list**.



4. Tap to select the screen idle time required before it refreshes to the home page.



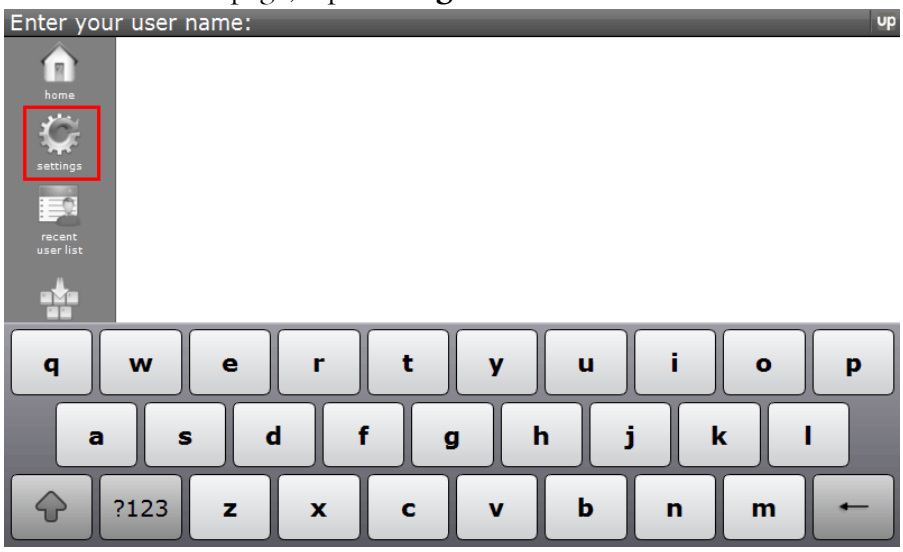
5. Tap **Apply**.

Changing Print Server Connection Information

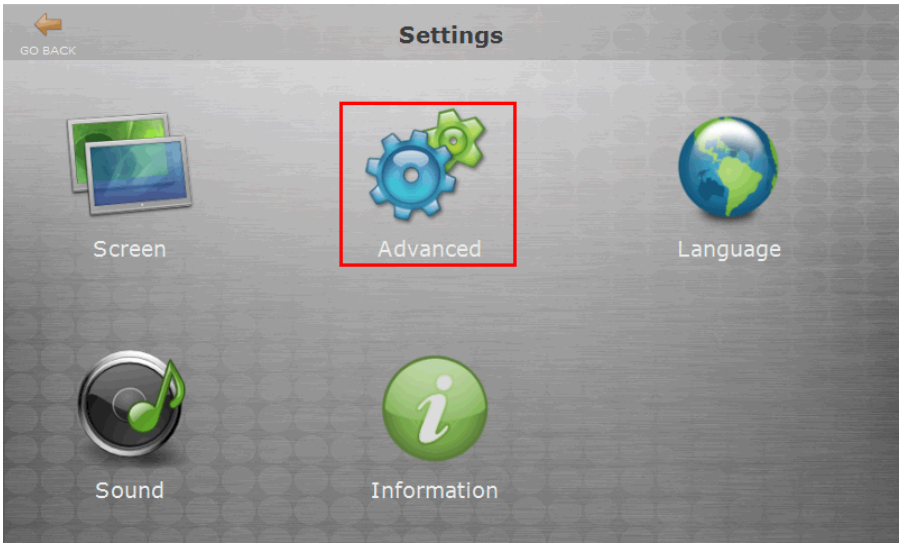
Although vPad automatically detects the closest UniPrint Print Server, it may still detect the incorrect server in a multiple UniPrint Print Server environment. This feature applies to the vPad Pro, vPad Touch and the SecurePrint emulator.

To change the Print Server connection IP address and port number, do the following:

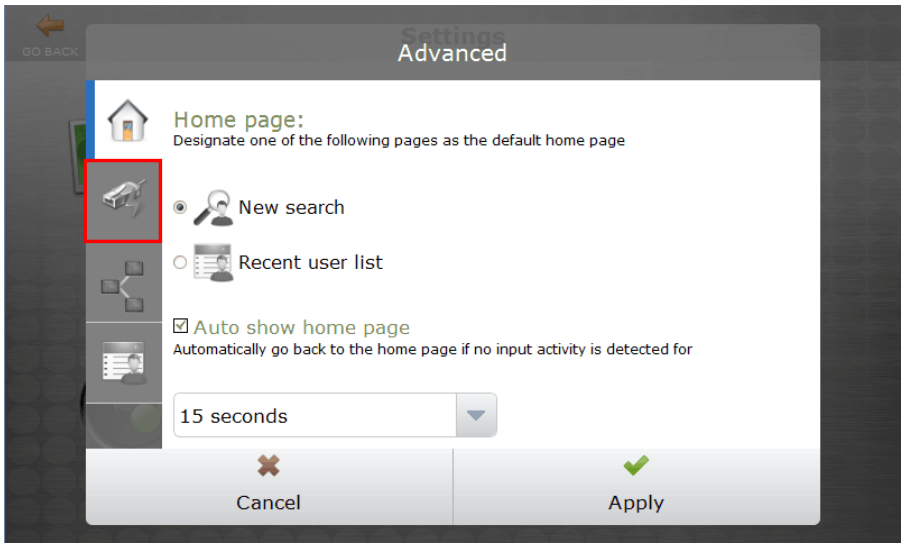
1. In the Home page, tap **Settings**.



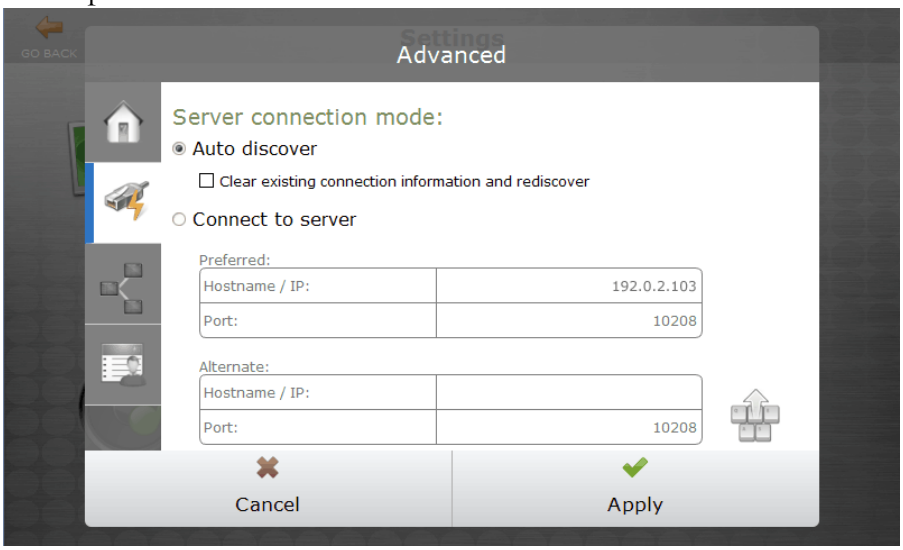
2. Tap **Advanced**.



3. Tap the **Network** tab.

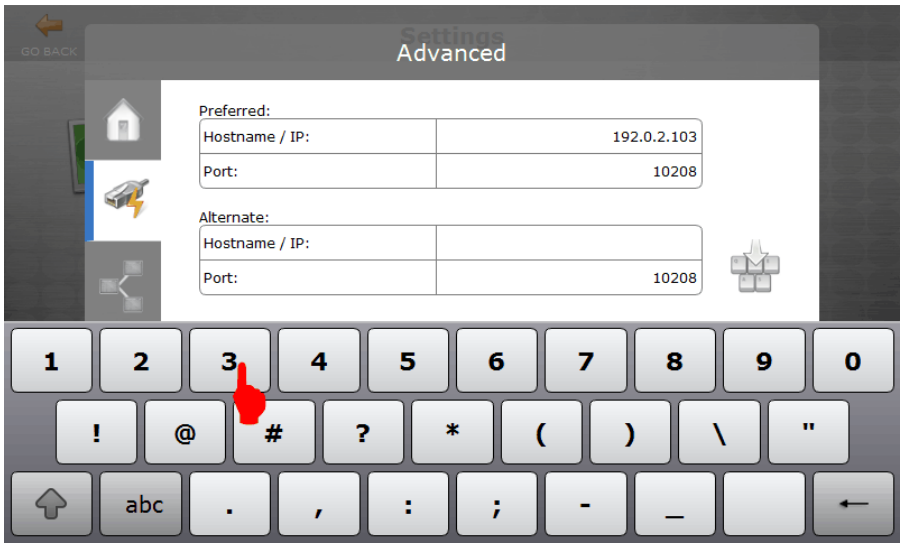


4. Tap either **Auto discover** or **Connect to server**.



a) If **Connect to server** is selected, tap within Hostname/IP and then tap the key pad to enter the new IP address and port number

of the UniPrint Print Server. An alternate print server can also be entered.

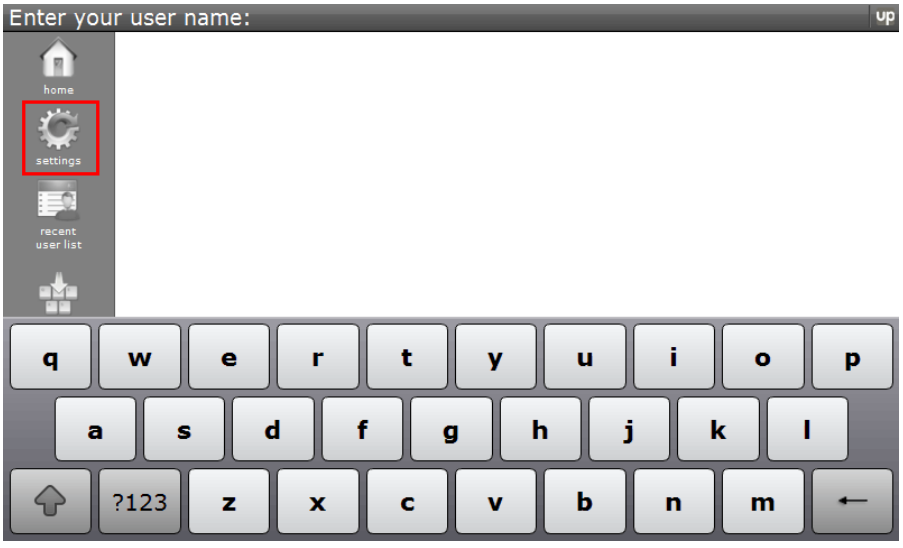


5. Click and then tap **Apply**.

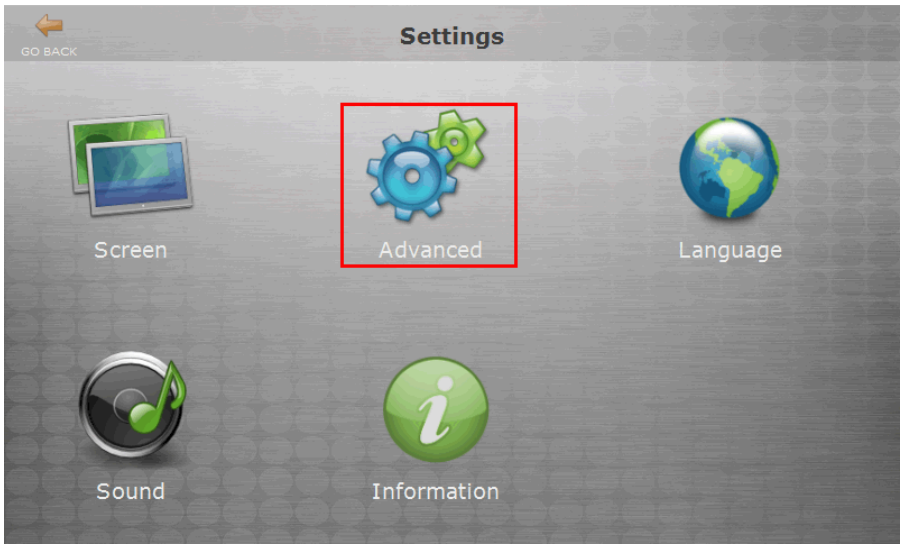
Assigning a Static IP Address To The vPad Pro

A static IP address can be assigned to the vPad Pro. This feature does not apply to the SecurePrint emulator or the vPad Touch, and the screen is therefore disabled.

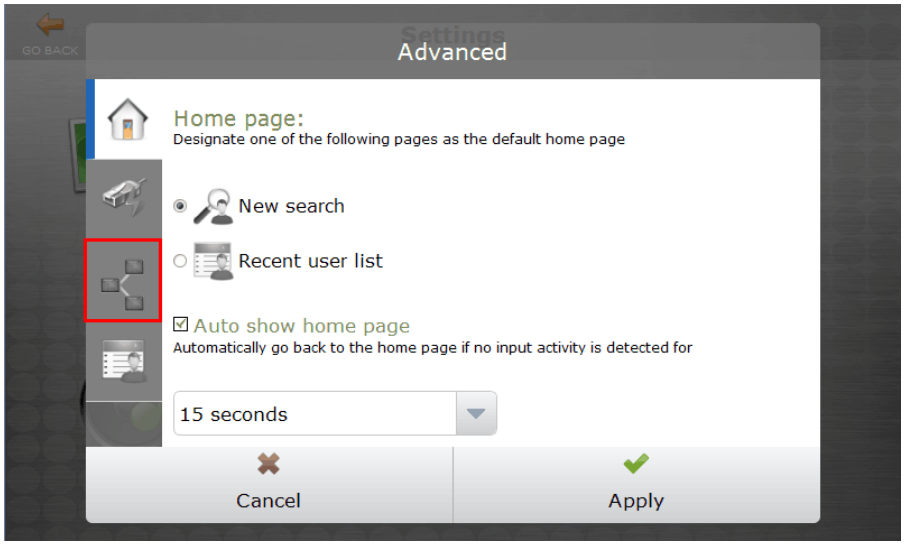
1. In the Home page, tap **Settings**.



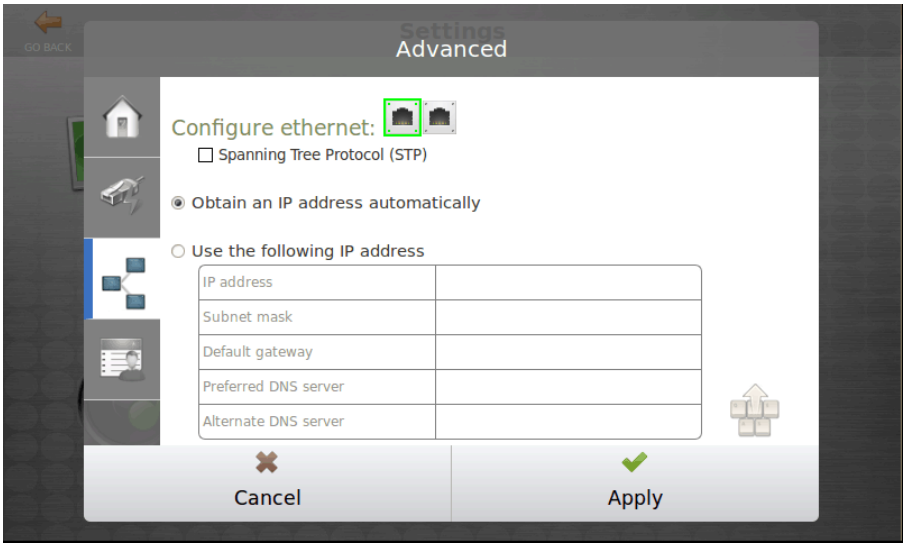
2. Tap **Advanced**.



3. Tap **Ethernet Connection** tab.

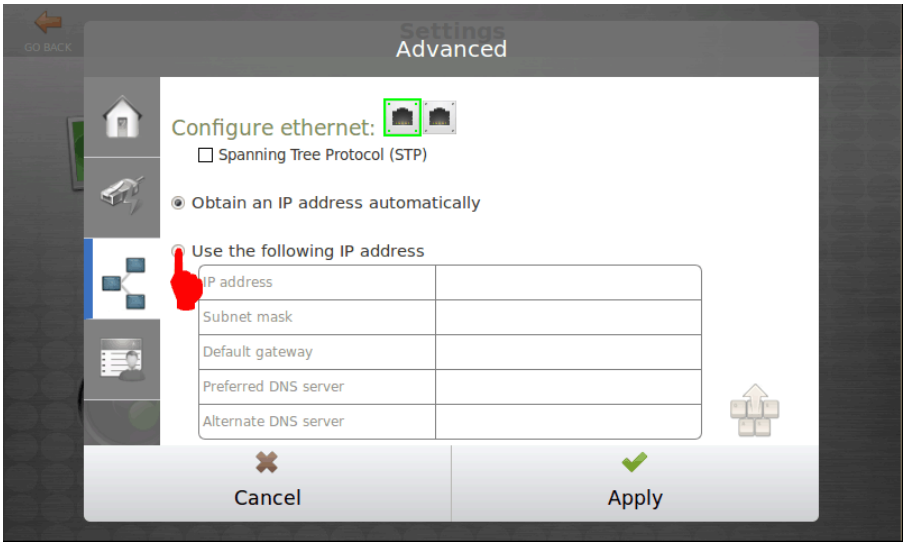


4. Ensure that the left ethernet port (highlighted in green) is used. This is the Ethernet port that is labelled eth1 and is used to connect to your network.

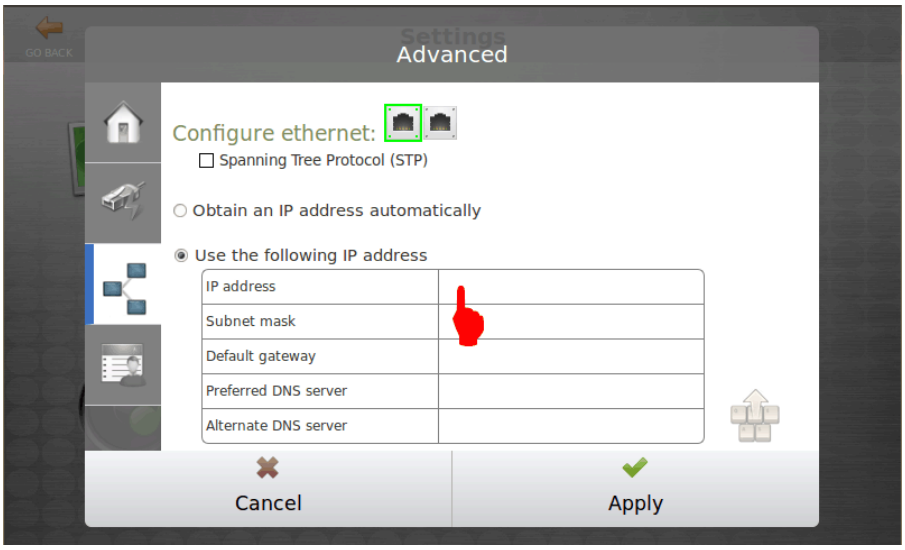


The non-green port which is labelled eth0 on the vPad Pro is used as a bridge when an additional network wall jack is unavailable for the vPad Pro. In this situation, disconnect the network printer from the network wall jack and connect it the vPad Pro on eth0. Then connect the vPad Pro to the network wall jack on eth1.

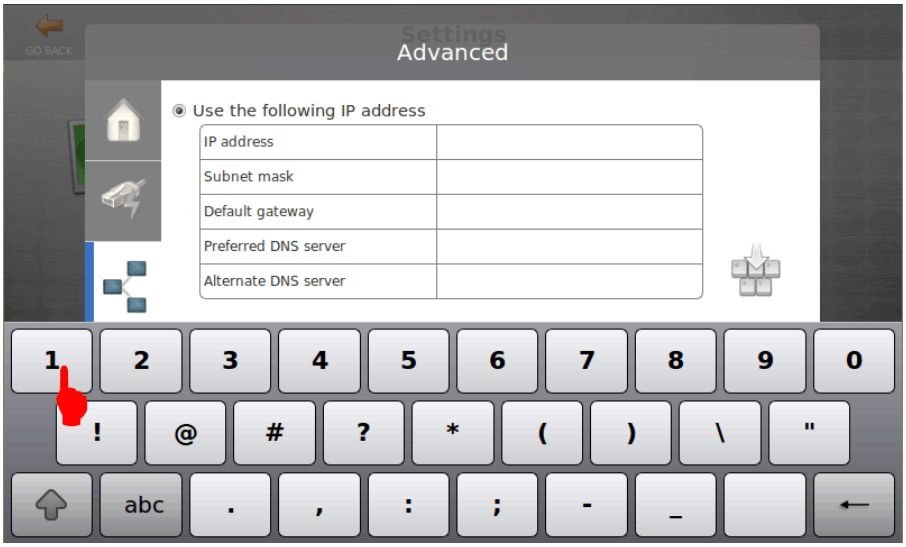
5. Tap **Use the following IP address**.



6. In the table, tap the empty cell beside **IP address**.



7. A keyboard will appear. Enter the IP address to be assigned to this device.



8. Tap the empty cell beside **Subnet mask** and then enter the appropriate IP address.

9. Repeat the above procedure to enter the **Default gateway**, **Preferred** and **Alternate DNS server** IP addresses.

10. Tap **Apply** when all the information is complete.

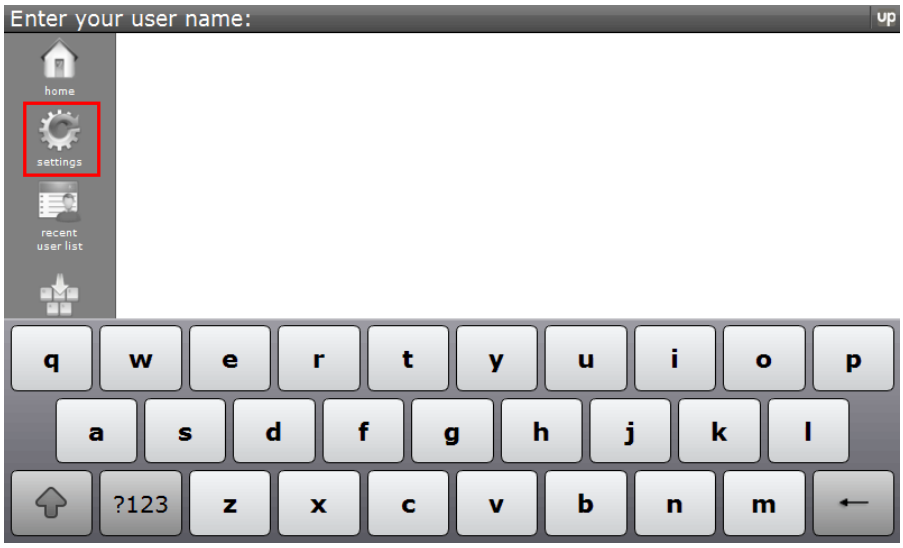
Changing the Number of Users Listed Under Recently Searched User Names

Users can also search for their user name in a list of **Recently searched users** instead of entering their user names each time. The number of users kept in

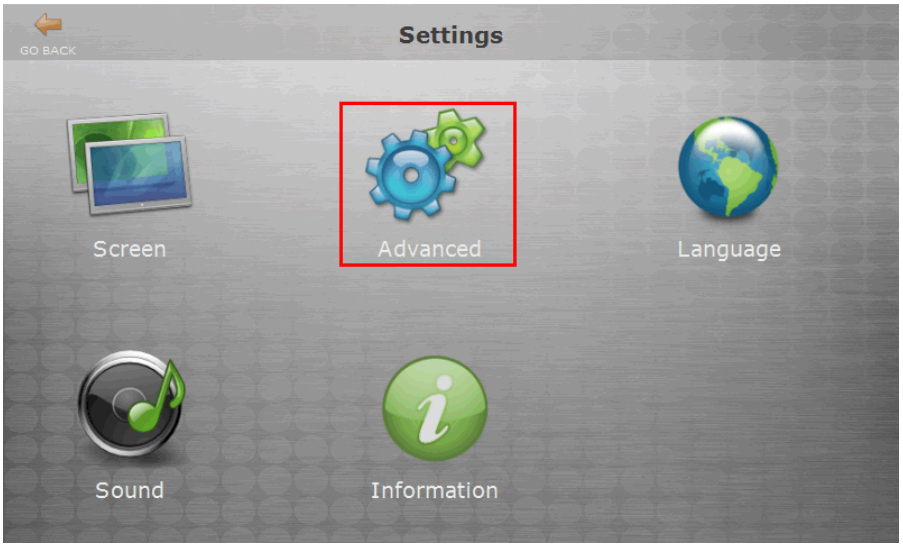
this list can be adjusted to meet your users' preference. This feature is applicable to the vPad Pro, vPad Touch and the SecurePrint emulator.

To change the number of users on the **Recently searched users** list, do the following:

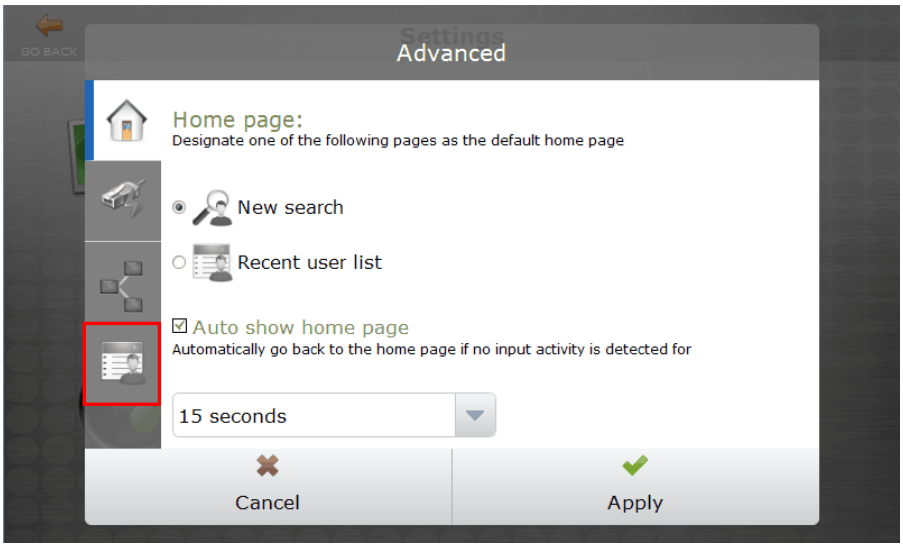
1. In the Home page, tap **Settings**.



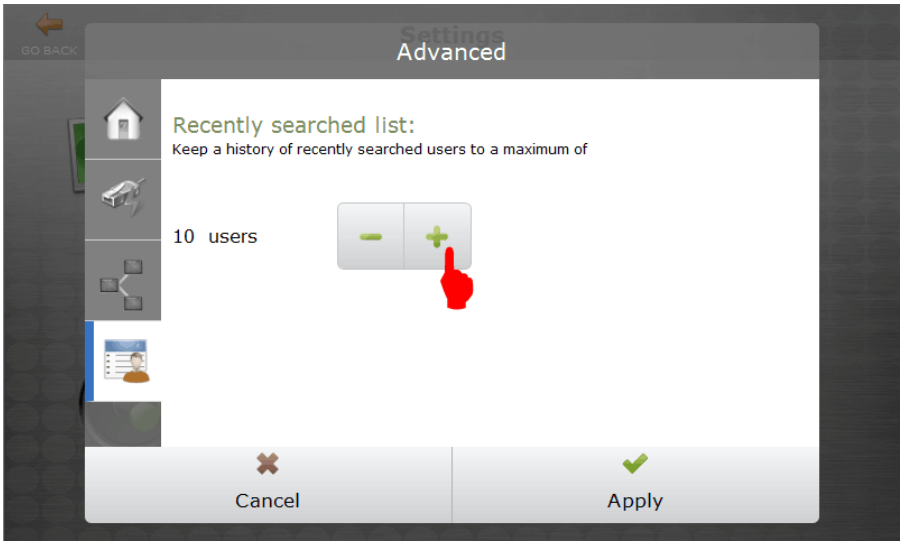
2. Tap **Advanced**.



3. Tap the **List** tab.



4. Tap the up and down arrows to adjust the number of users kept in the search list.

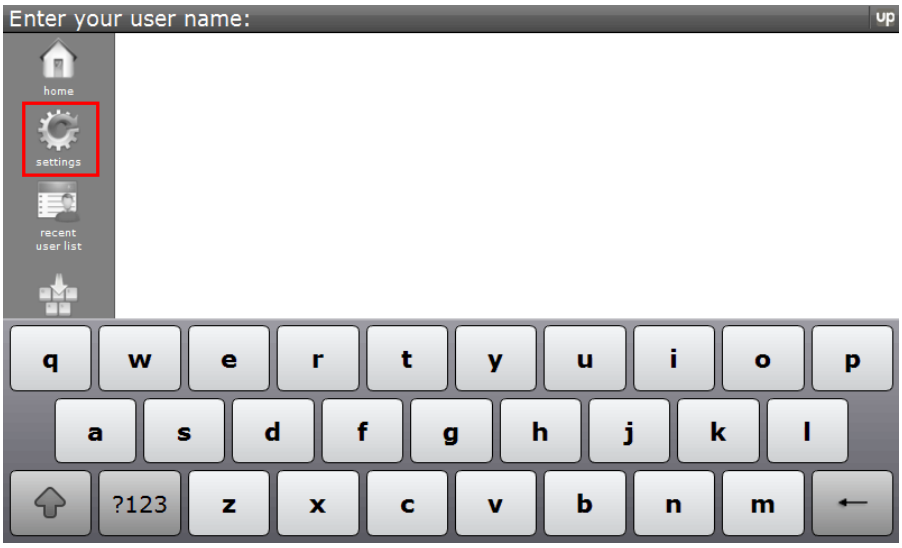


5. Tap **Apply**.

Changing the Interface Language

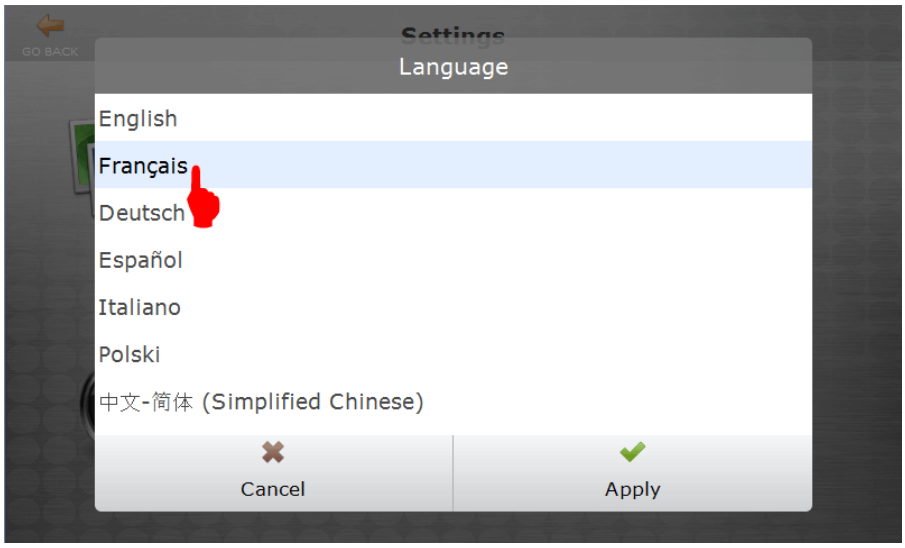
Currently, the vPad Pro, vPad Touch and SecurePrint emulator interfaces support English, French, German, Spanish, Italian, Polish and simplified Chinese. However, provisions have been made to include other languages in future releases. To change the interface language, do the following:

1. In the Home page, tap **Settings**.



2. Tap **Language**.

3. Tap to select a language.



4. Tap **Apply**.

5. Tap **Yes** to confirm that you want to change the interface language.

NOTE: After changing the interface language, extended latin-derived characters such as accents and ligatures can be accessed by pressing and holding a key:

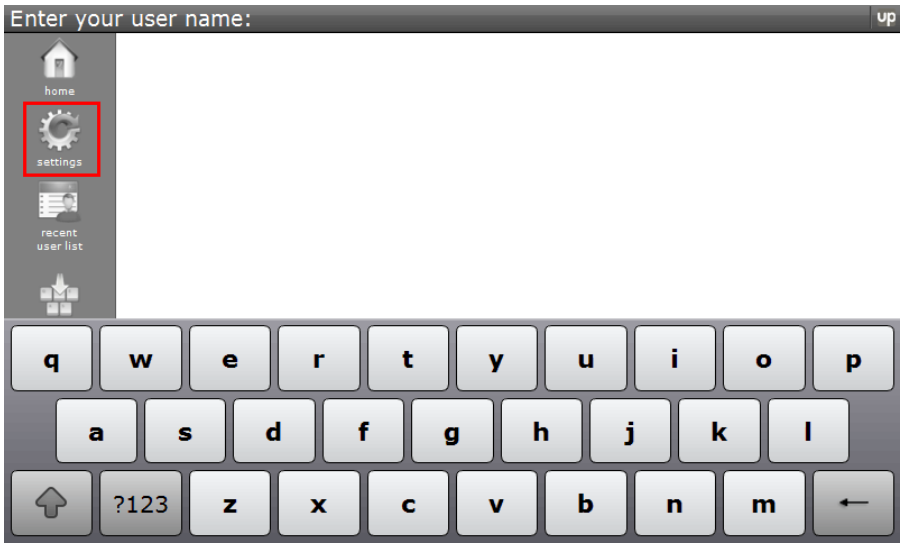
For example, if the interface language is set to French, pressing and holding A would allow for A with accent grave, circumflex, tréma, and the AE ligature.

Adjusting Sound and Volume

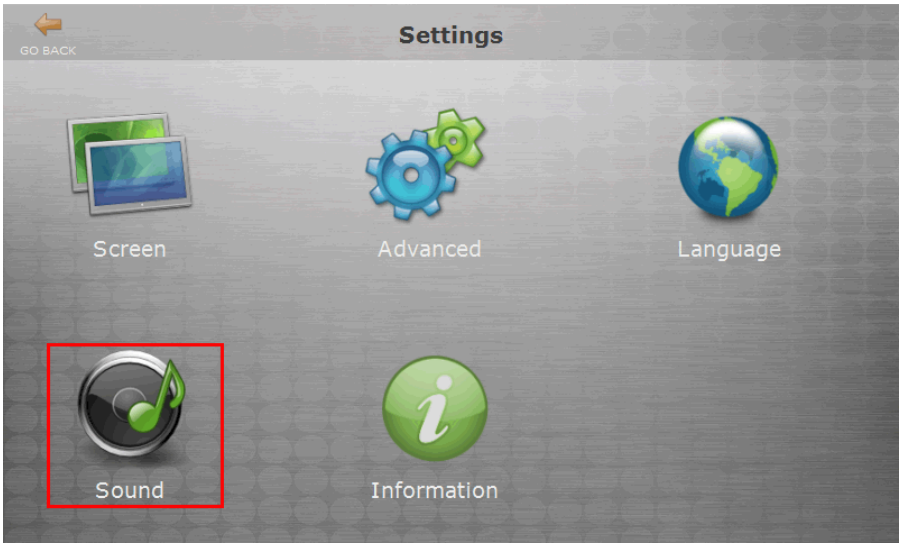
This feature only applies to the vPad Pro and does not apply to the SecurePrint emulator, vPad Touch or vPad CE. To adjust the sound and volume for the SecurePrint emulator or vPad Touch, use the Control Panel in Windows.

To change the sound and volume, do the following:

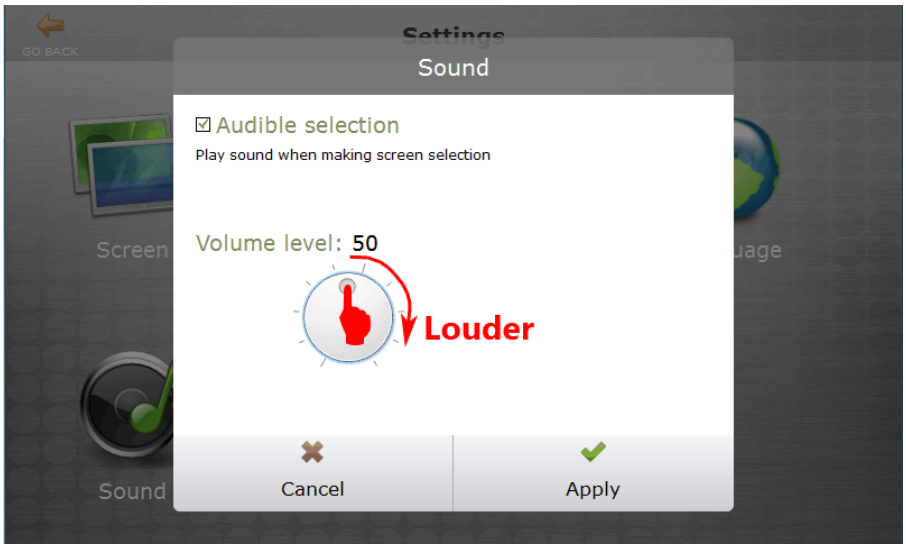
1. In the Home page, tap **Settings**.



2. Tap **Sound**.



3. Press, hold and drag the volume wheel to adjust the volume level.

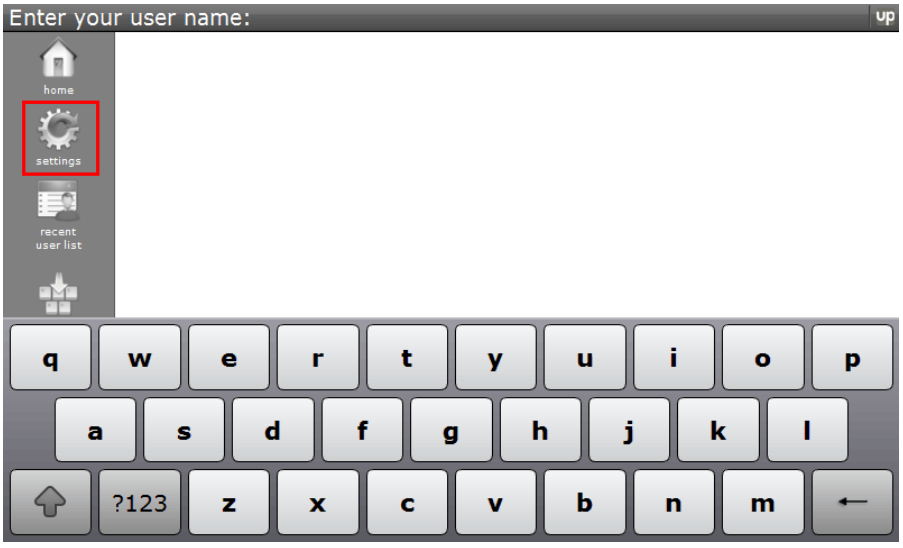


4. Tap **Apply**.

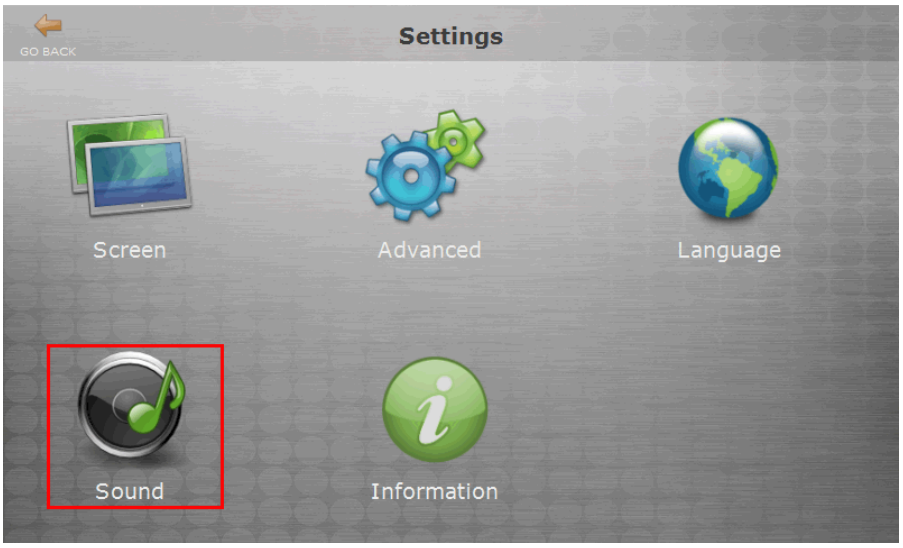
Muting Tap Sounds

To mute the tap sounds, do the following:

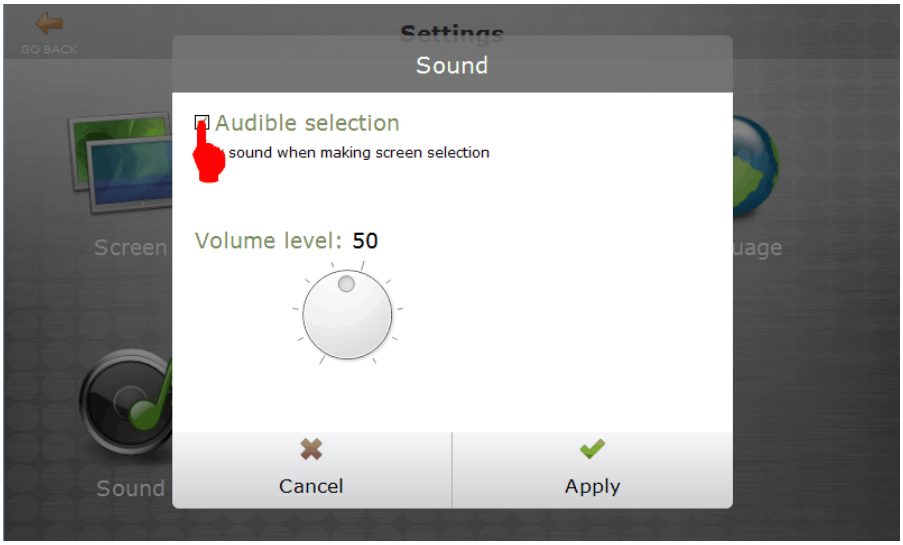
1. In the Home page, tap **Settings**.



2. Tap **Sound**.



3. Tap to clear **Audible selection**.



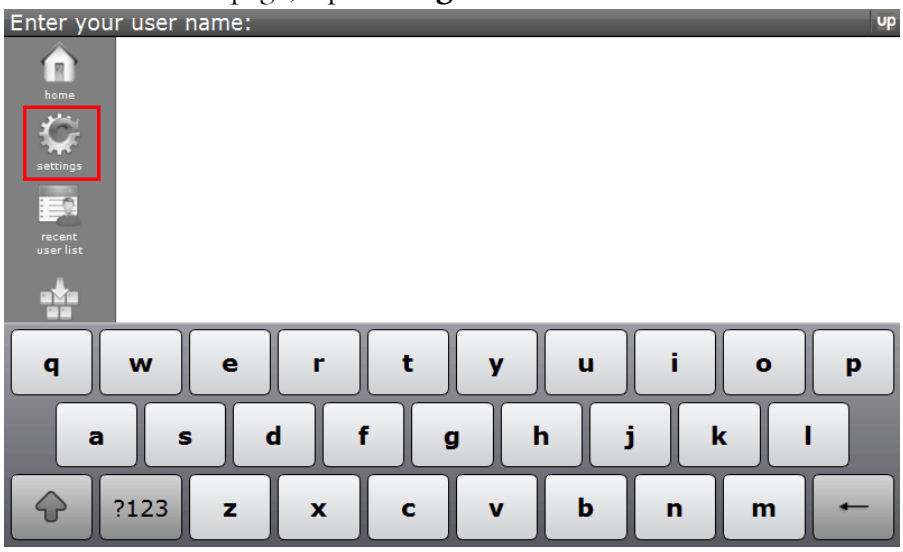
4. Tap **Apply**.

Retrieving Information About the vPad

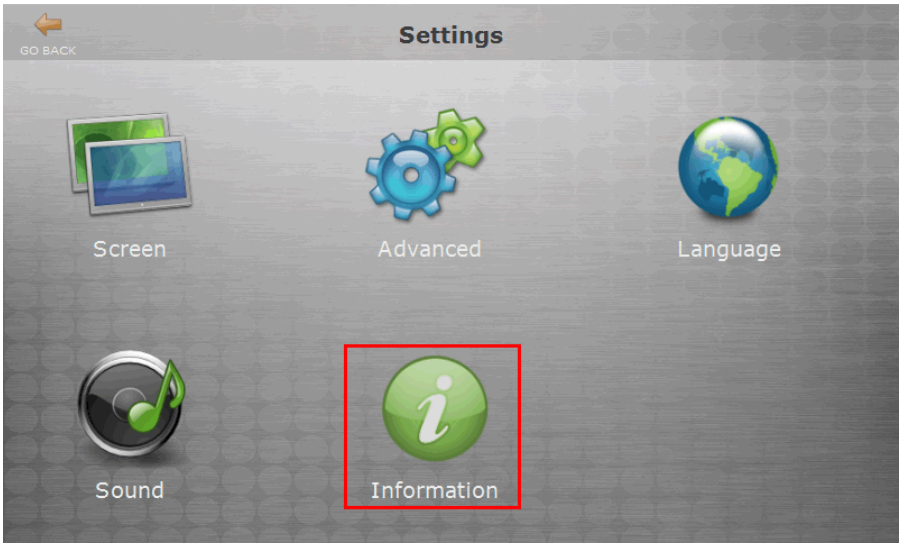
From the vPad Information screen, you can find out how much free memory is available, the device's IP address and which UniPrint Print Server it is connected to. This feature is available for all vPad devices and the SecurePrint emulator.

To learn more about your vPad, do the following:

1. In the Home page, tap **Settings**.



2. Tap **Information**.



3. Review the information and then tap **Close**.

4. If an alternate print server has been entered or if High Availability has been implemented, 2 print servers will be presented. The green IP address is the active print server. Tap **Close**.

Configuring Printer Delegation

At times, users may want to delegate their print jobs to others to avoid having to e-mail documents that require printing. Print jobs can be delegated to a group of users that are set up by the administrator or users can delegate print jobs on the fly depending on how delegation is configured.

With print job delegation, the user(s) to whom the print job is delegated to receive an e-mail message that contains a randomly generated 4-digit PIN

code. The user(s) authenticate on the vPad, select the delegated print job and then use the PIN code to release it for printing to a physical printer.

Setting up Email Server Settings for Printer Delegation

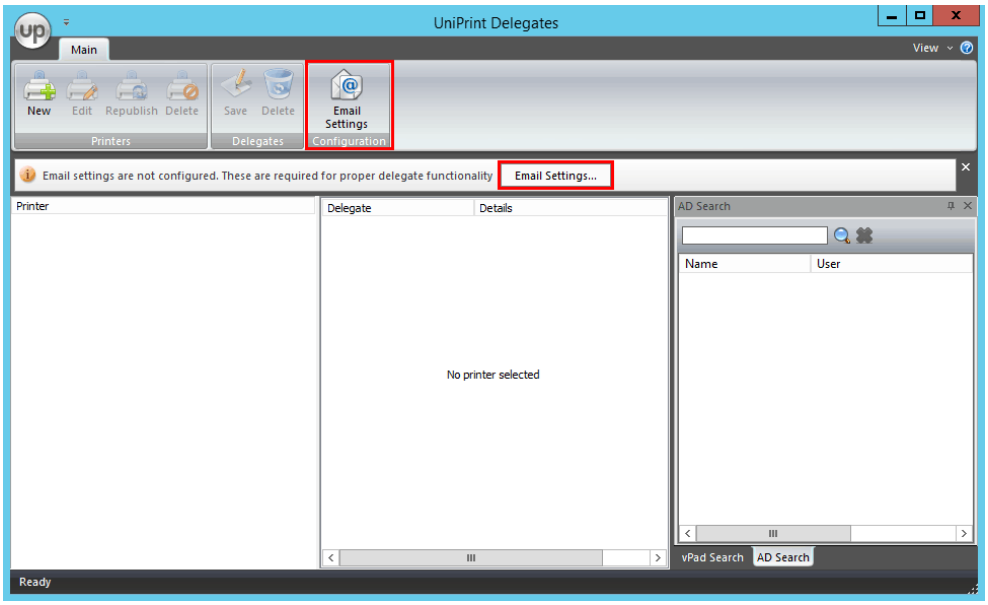
Since users are notified of print job delegation and status through e-mail, e-mail settings need to be set.

To configure e-mail settings, do the following:

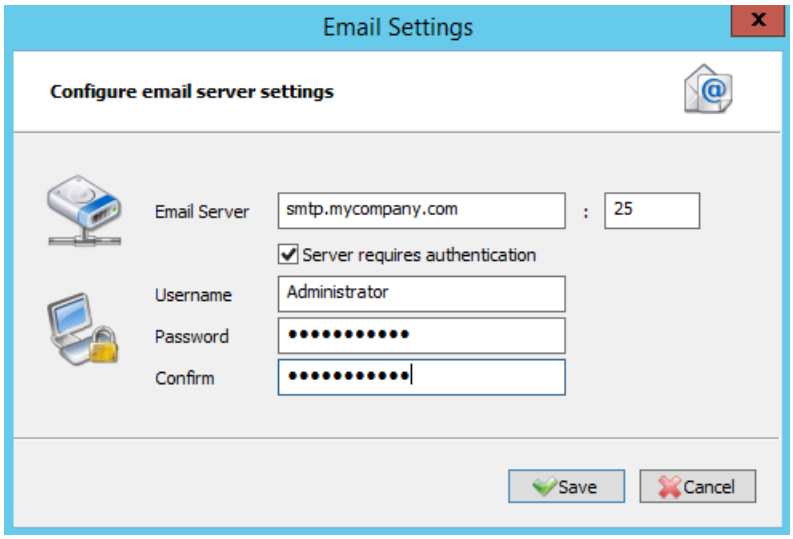
1. On the **SecurePrint Server** (UniPrint Bridge), click **Start** and the type `Delegates`.

2. Click **Delegates**. ***Note:*** *If Delegates is to be accessed frequently, it is recommended that Delegates be pinned to either the taskbar or to Start.*

3. Click **Email Settings**.



4. Enter in the e-mail server information and if necessary, server credentials. Click **Save**.



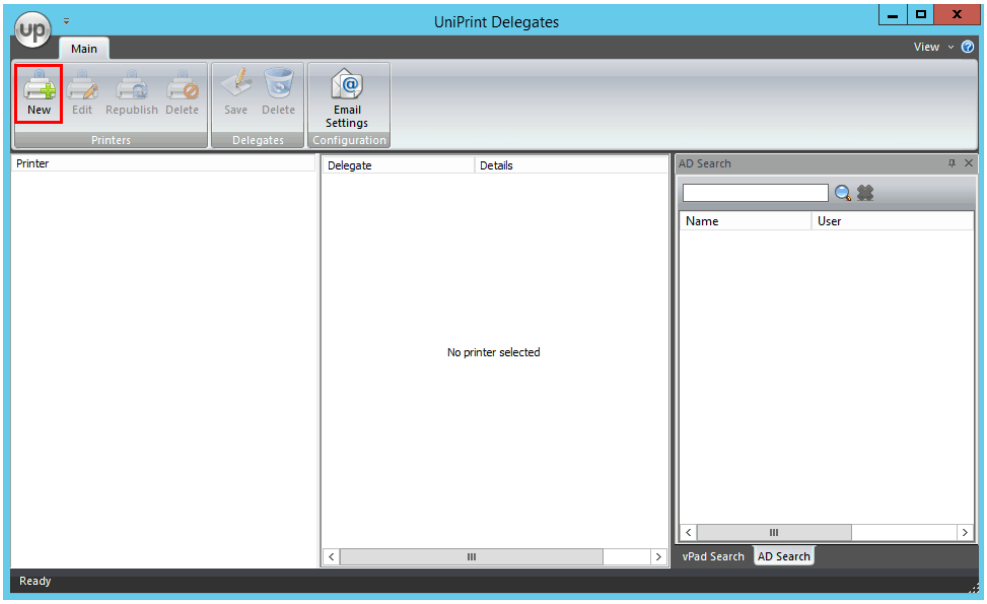
Creating a New Delegate Printer Queue

Delegate printer queues can be created based on a project, a department or even a job function, for example. It really depends on how this functionality will be used in your users' work flows.

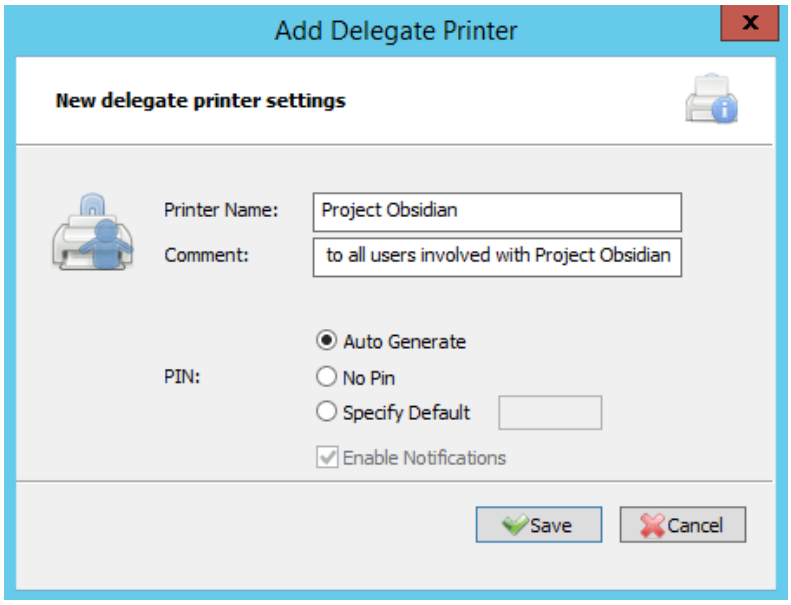
To create a new delegate printer queue, do the following:

1. On the SecurePrint Server (UniPrint Bridge), open **Delegates**.

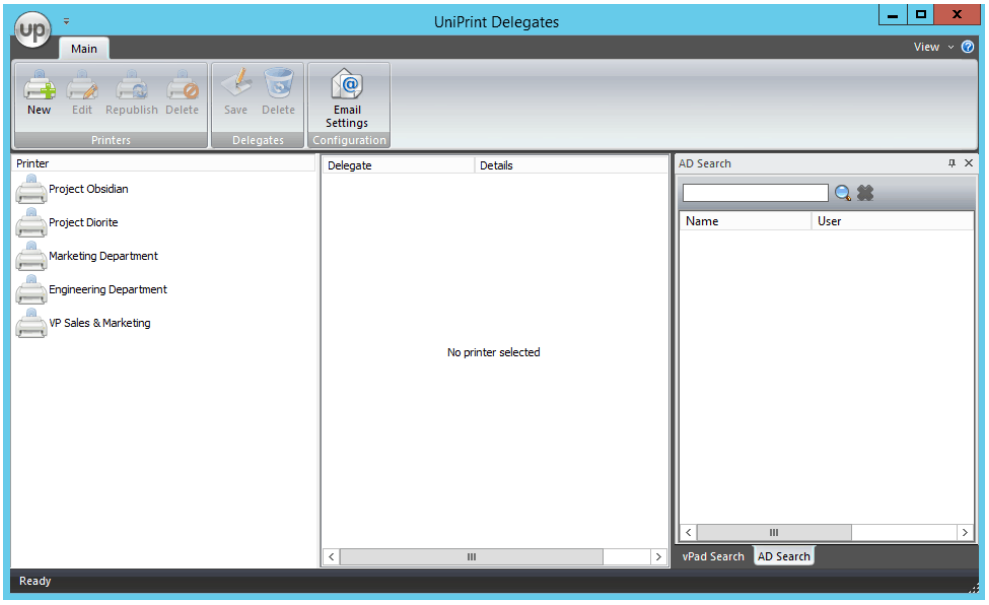
2. Click **New** to create a delegate printer queue.



3. Type in the name of the new delegate printer, a comment, and also select how the SecurePrint password/PIN will be created. A 4-digit SecurePrint PIN can be automatically generated, no PIN can be generated or the administrator can set a pre-defined PIN. This PIN is required by the delegate user to release the print job. Click **Save**.



4. The new delegate printer queue is created and will be published to the UniPrint Bridge. Continue to create as many delegate printer queues as required.



Assigning Delegates and vPads to a Delegate Printer Queue

There are 2 types of printer delegation queues, administrator-initiated and user-initiated. With administrator-initiated queues, the administrator assigns

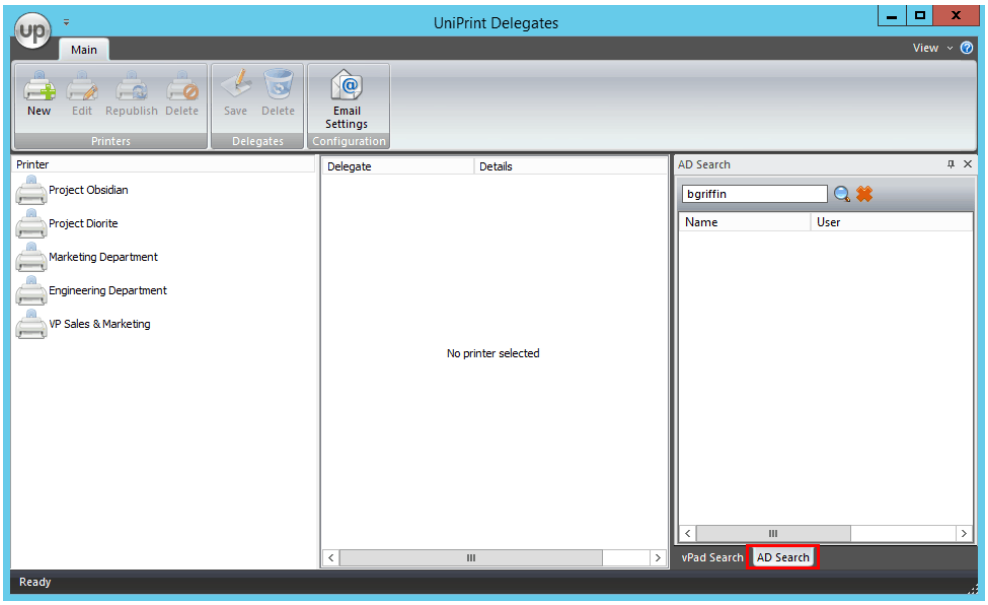
delegates and vPads to the queue. Whereas with user-initiated queues, the user delegating the print job assigns the delegates at the time of printing.

For user-initiated queues, leave the delegates list blank.

NOTE: A new feature in version 9.1, is vPad delegation for administrator-initiated queues. Administrators can assign not only users, but also vPads to a delegate printer queue. By the adding a vPad to the queue, users receive an e-mail with the SecurePrint PIN, but they can only release the print job at the delegated vPad. If the user attempts to release the print job at a non-delegated vPad, the print job will still appear in their print job list after they authenticate with their domain credentials, however the **Print** and **Print Direct** buttons will be disabled.

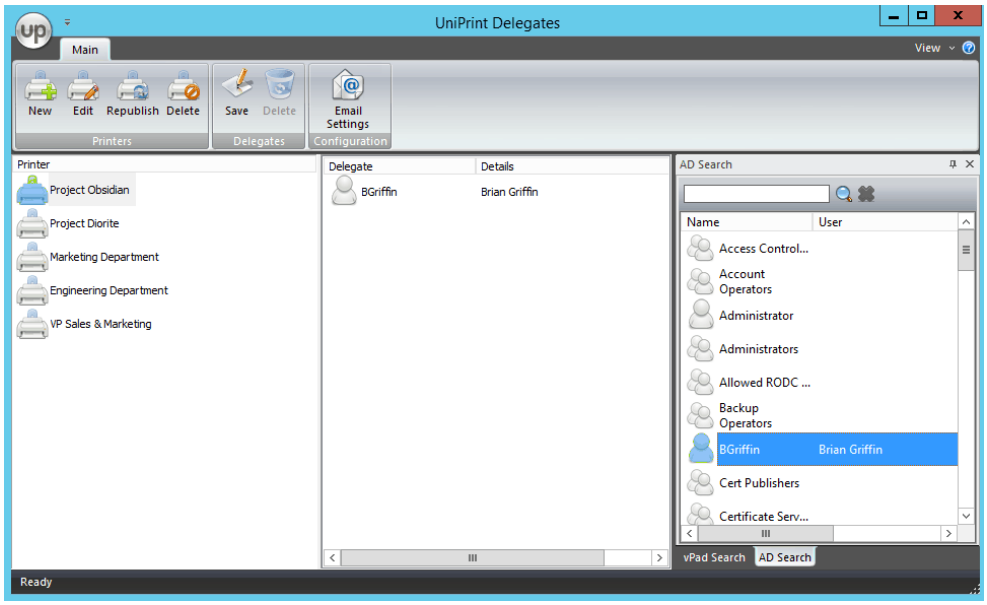
For administrator-initiated queues, do the following:

1. On the SecurePrint Server (UniPrint Bridge), open **Delegates**.
2. Click to select a delegate printer queue.
3. Click the **AD Search** tab, under **Search**, type in a domain user name and then click .



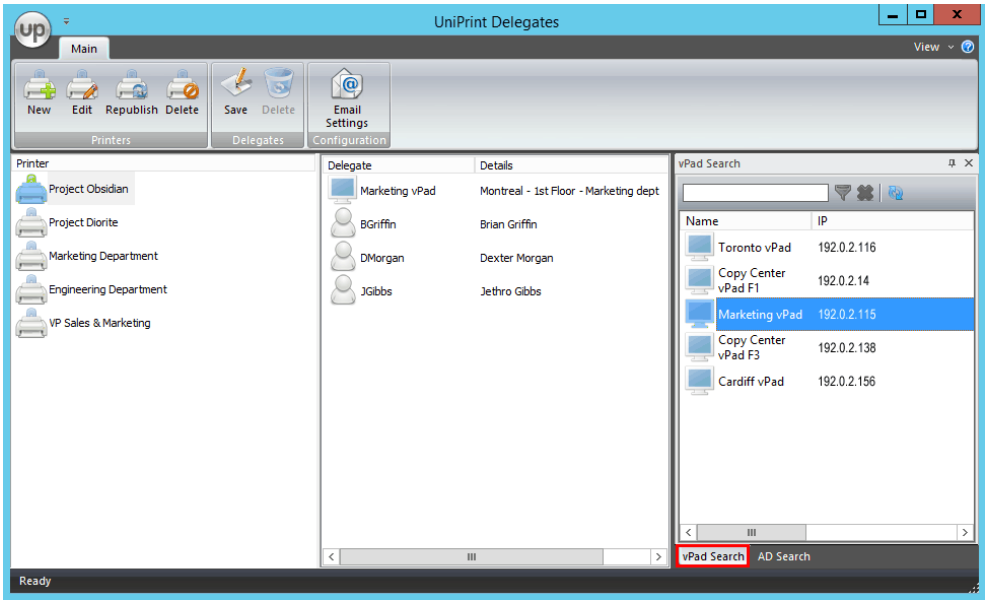
To populate the user list with all domain users, leave the search box blank and click . ***Note**: The user list may take a long time to populate if your Active Directory is large.*

4. Click to select a user and then press **ENTER** to add them to the delegates list.

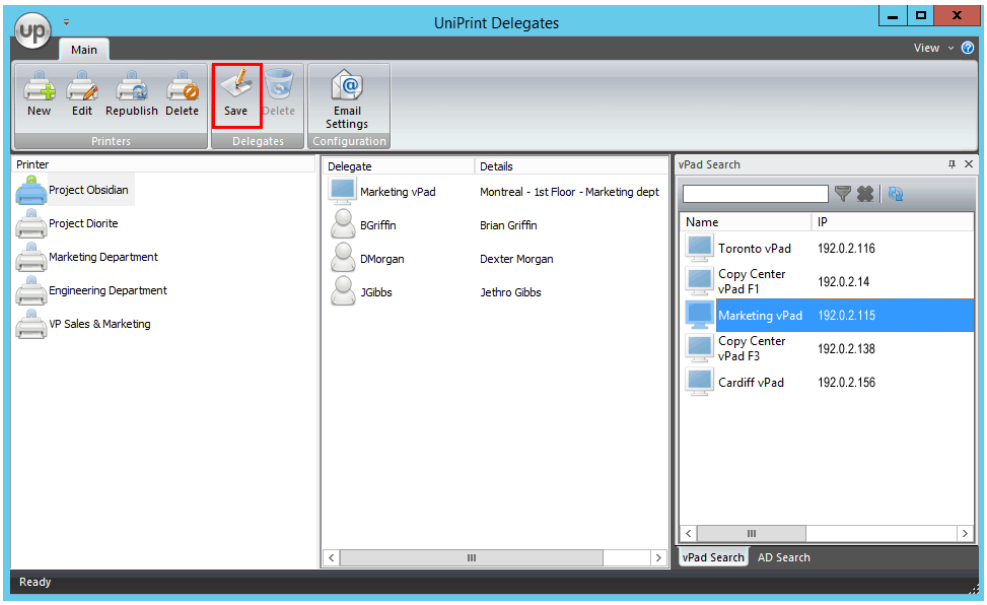


NOTE: To add multiple users that appear consecutively in the list, click the first user you want to add, press **SHIFT** and then click the last user. Press **ENTER** to assign them to the delegation queue. To add multiple users that do not appear consecutively in the list, click to select a user, press **CTRL**, and then click the next user. Press **ENTER** to assign the users to the delegation queue.

5. To delegate a vPad, click the **vPad Search** tab. Click to select the vPad and then press **ENTER**.



6. Click **Save**.

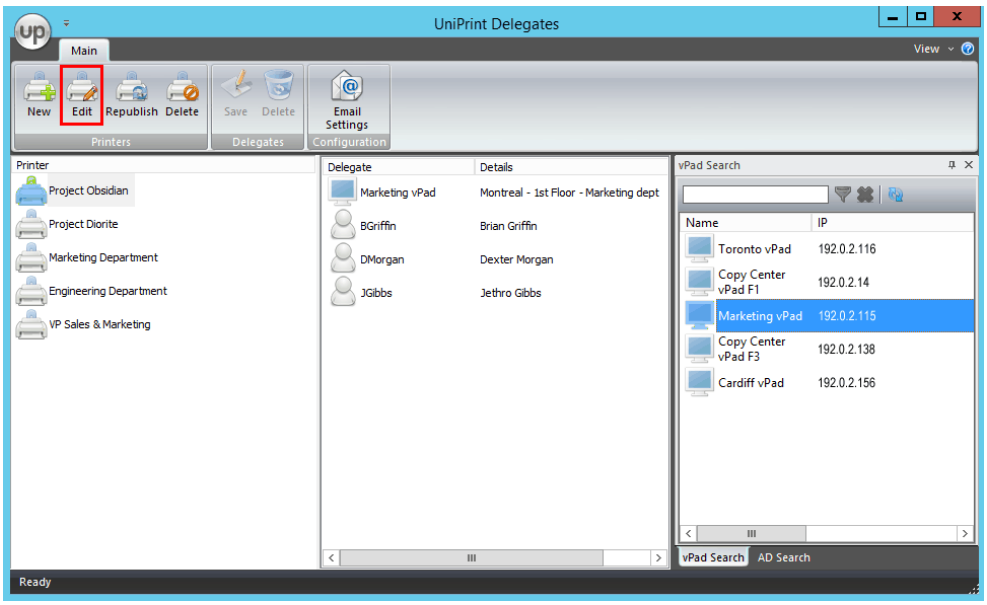


Modifying a Delegate Printer

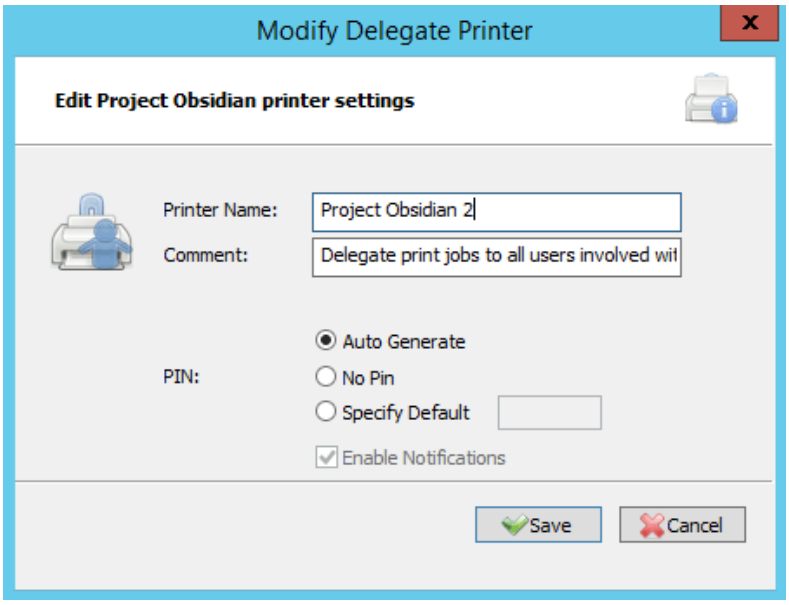
To modify the delegate printer name and/or comments, do the following:

1. On the SecurePrint Server (UniPrint Bridge), open **Delegates**.

2. Click to select a delegate printer and then click **Edit**.



3. Edit the printer name, comments, PIN creation option and then click **Save**.

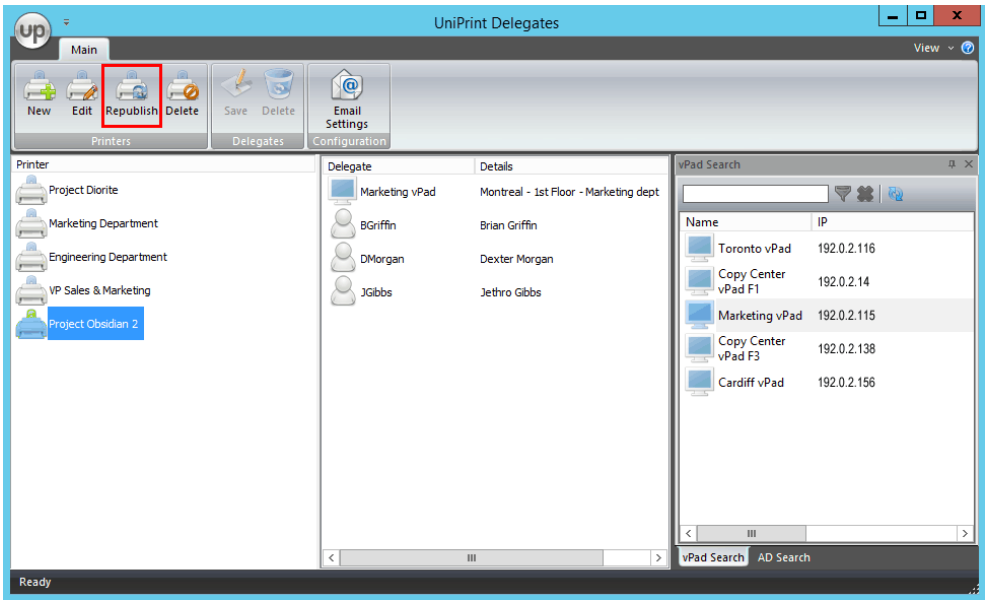


Republishing a Delegate Printer to the Bridge

If a delegate printer has been deleted on the UniPrint Bridge, it can be republished by doing the following:

1. On the SecurePrint Server (UniPrint Bridge), open **Delegates**.

2. Click to select a delegate printer and then click **Republish**.



3. Click **Yes** to confirm that you want to republish the printer to the UniPrint Bridge.

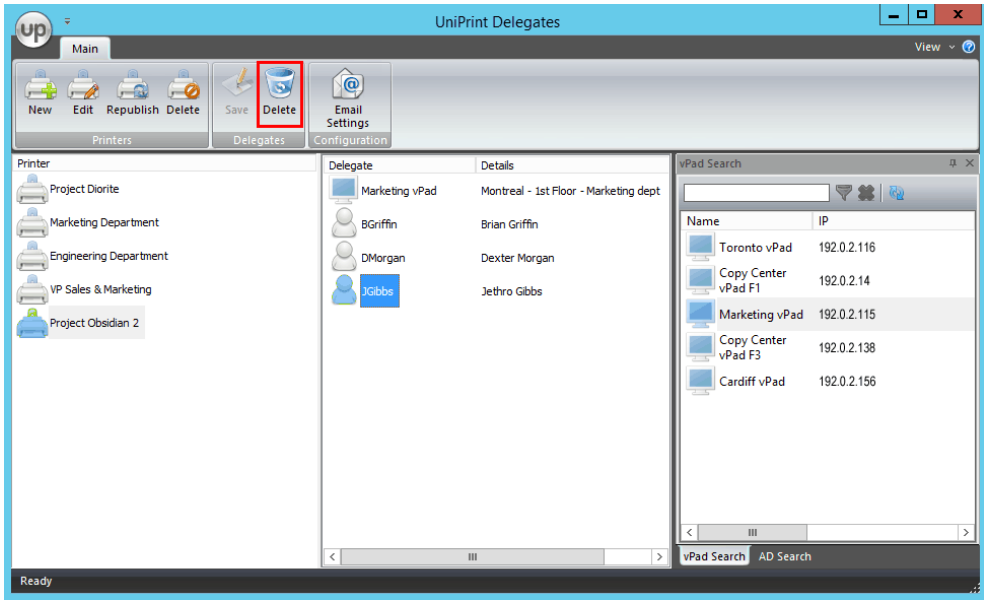
Deleting a User or vPad From The Delegates List

To remove a user or vPad from the printer delegation list, do the following:

1. On the UniPrint Bridge, open **Delegates**.

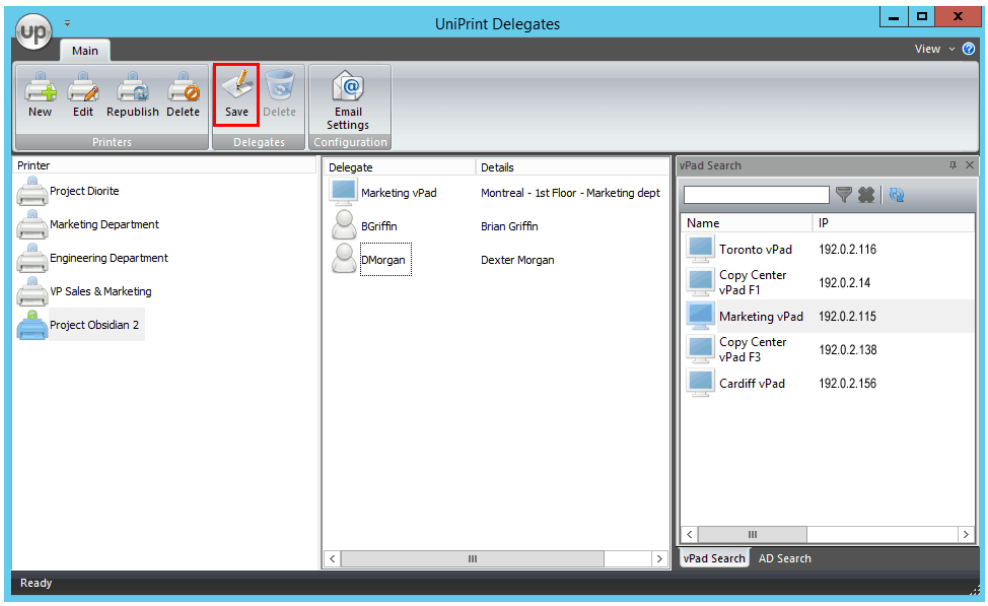
2. Click to select a delegate printer.

3. Click to select the user or vPad in the delegation list and then click **Delete**.



4. Click **Yes** to confirm that you want to delete the selected delegate.

5. Click **Save**.

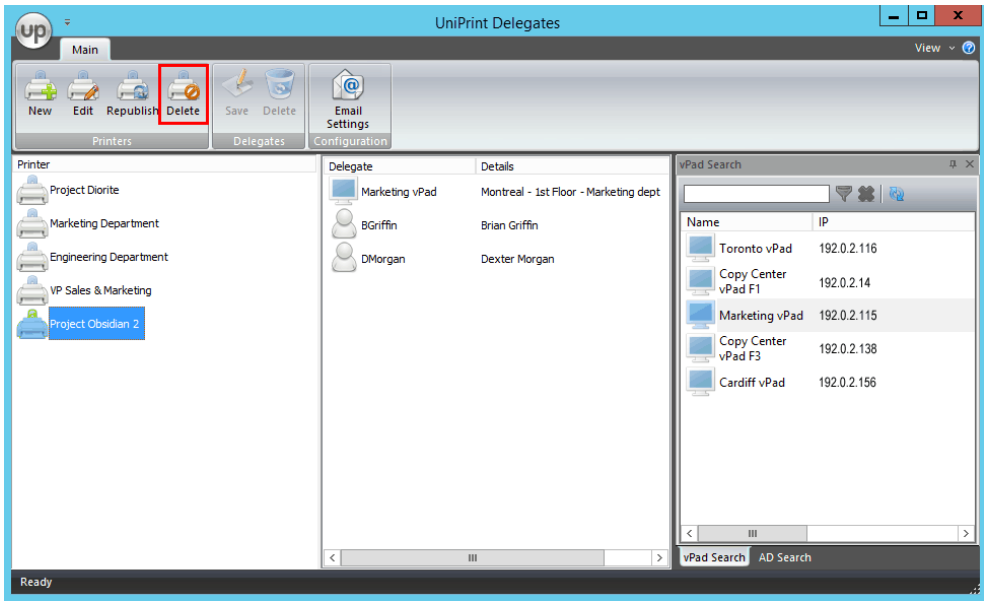


Deleting a Delegate Printer Queue

To delete a delegate printer queue and all of its delegates, do the following:

1. On the UniPrint Bridge, open **Delegates**.

2. Click to select a delegate printer queue and then click **Delete**.



3. Click **Yes** to confirm that you want to delete the delegate printer and all of its delegates.

Delegating a Print Job

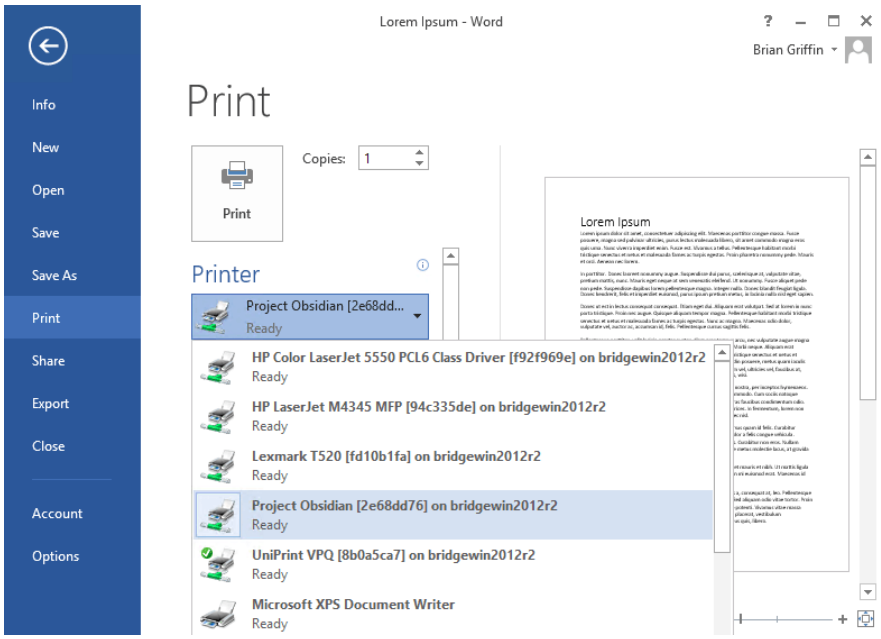
Once printer delegation has been configured, the user can then delegate print jobs to either admin-initiated queues or to user-initiated queues. With admin-initiated queues, the print job is automatically delegated to the users assigned to the queue by the administrator. For user-initiated queues, the user will be prompted to enter the user names who are to be delegated the print job at the time of printing.

Delegates will receive an e-mail message with a 4-digit, randomly generated, PIN code, notifying them that a print job has been delegated to them. Delegates can then proceed to a vPad device, authenticate and then enter this PIN code to release the delegated print job to a printer.

To delegate a print job, do the following:

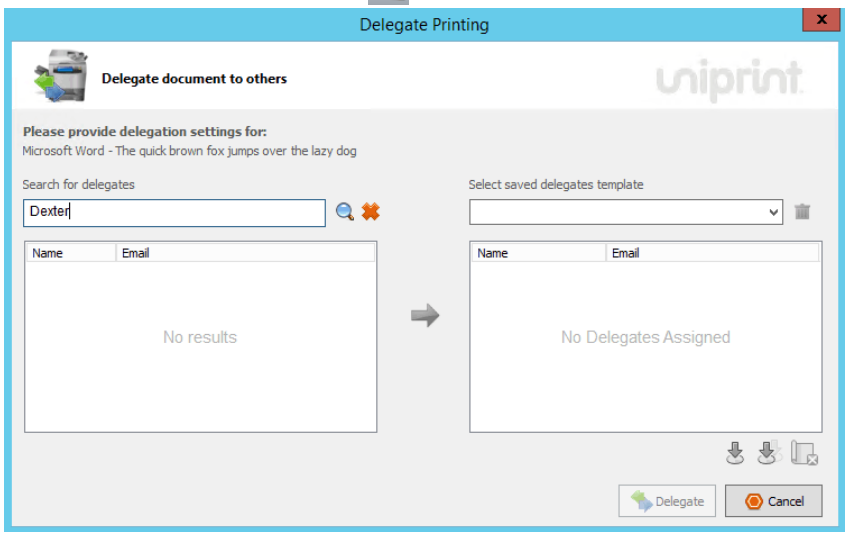
1. In an ICA/RDP session, open an application and then click **Print**.

2. Select a delegate printer and then click **Print**. For admin-initiated

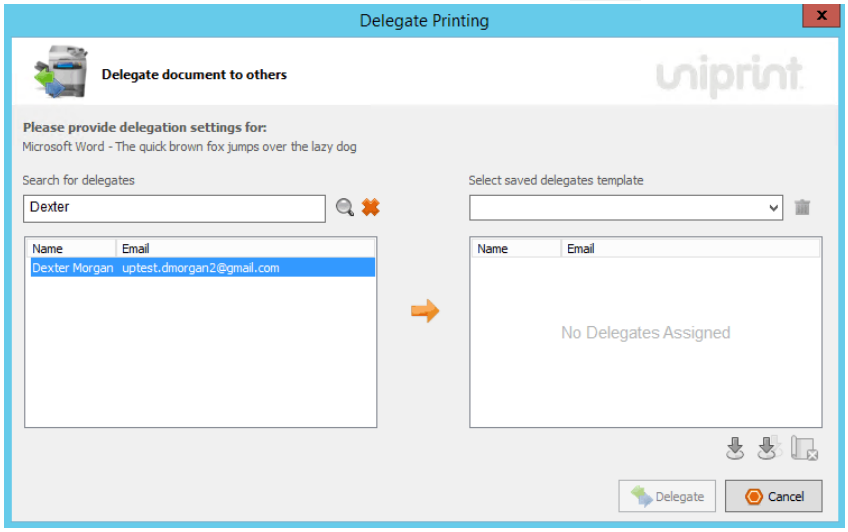


queues, an e-mail will be sent to the delegates notifying them that a print job has been delegated to them along with a 4-digit PIN that is to be used to release the print job to a printer.

3. For user-initiated queues, you will be prompted for delegates. Type in a username and then click .

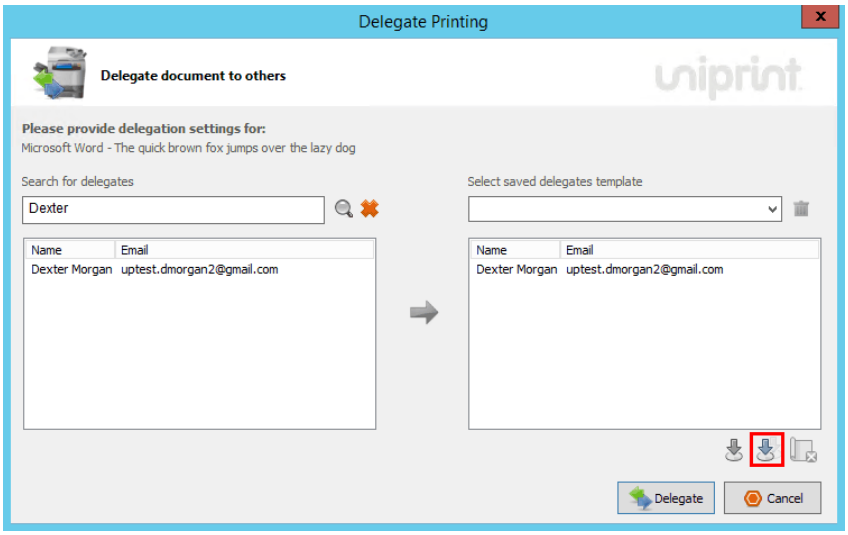


4. Click to select the delegate and then click .

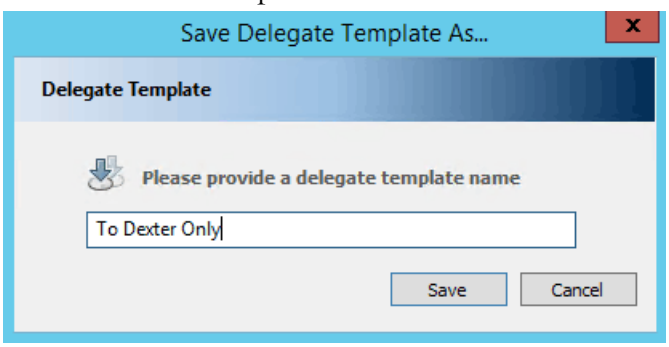


5. Continue to search for and select delegates as needed.

6. To save your delegates as a template, click .

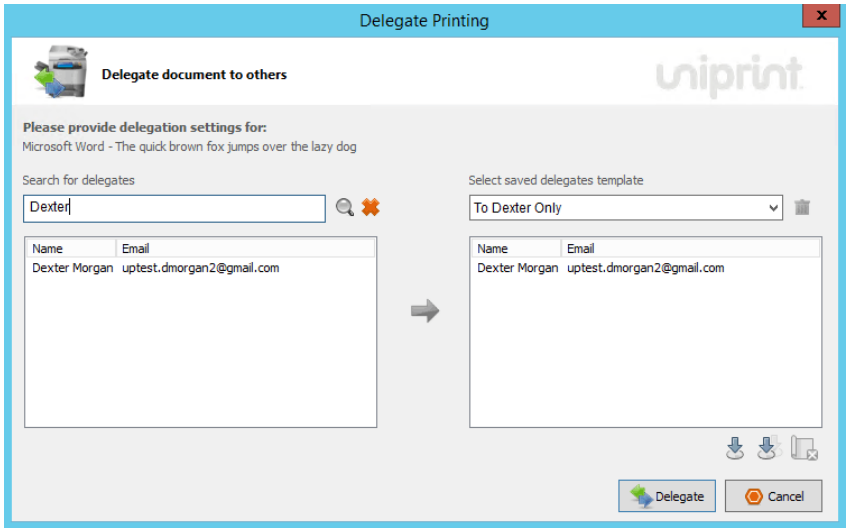


7. Enter a name for the template and then click **Save**.



8. To remove a delegate from a template, click to select the delegate and then click . To save changes to an already existing template, click .

9. To delegate the print job, click **Delegate**.



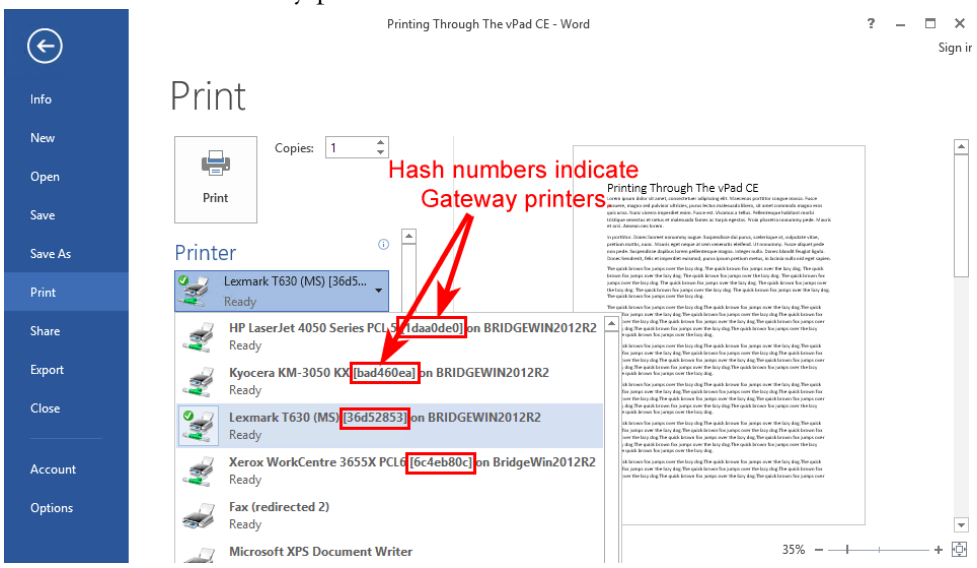
10. An e-mail will be sent to the delegate(s) notifying them that the print job is ready to be retrieved.

Printing through the vPad CE

Unlike the vPad Standard, Pro and Touch models, the vPad CE lacks a display. However, pull printing is still possible by using the vPad CE with an external or internal card reader. Instead of entering a SecurePrint password to release a print job, the user simply taps their RFID/HID card on the vPad CE device to release the print job. The vPad CE also enables print stream compression.

1. In an ICA/RDP session, open an application and then click **Print**.

2. Select a Gateway printer and then click **Print**.

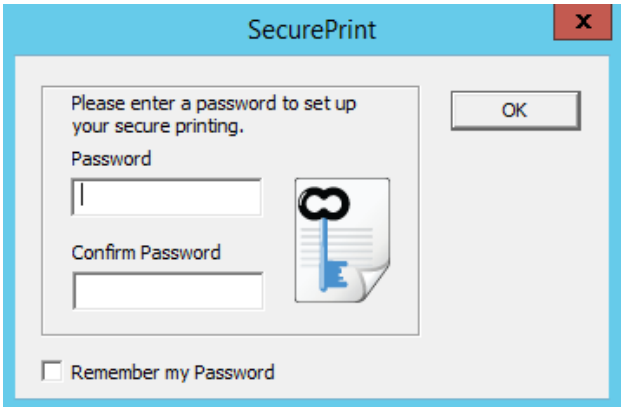


3. The print job will be compressed at the central print server and then decompressed by the vPad CE before being printed at the printer. Since print stream compression is configured on the print server through the UniPrint Transport Port Monitor, print stream compression and decompression appears seamless to the user.

4. If the vPad CE with an internal/external card reader is used, the print job will be released to printer that is associated with it on the UniPrint Management Console.

Setting up your SecurePrint Password

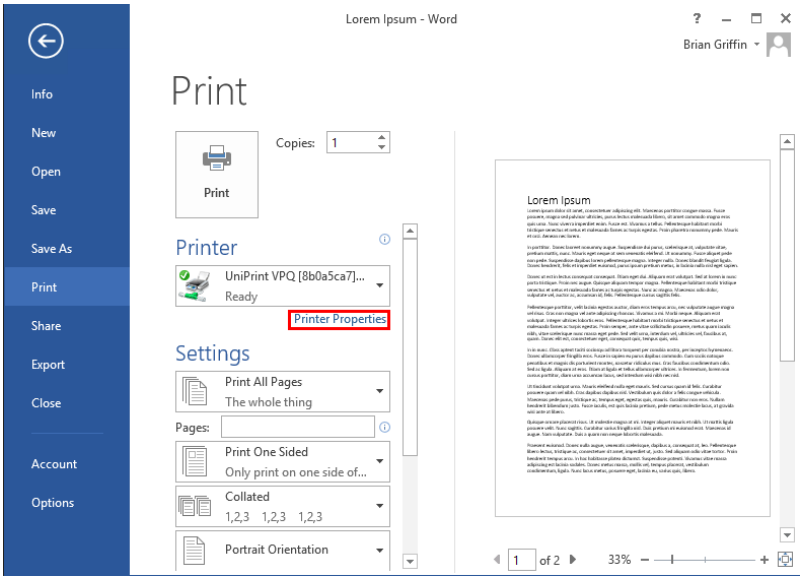
If Force Password is enabled, the user will be required to enter a password each time they print to the UniPrint VPQ or any Gateway printer.



If Force Password is not enabled, then to set up a password the user needs to do the following:

1. In an ICA/RDP session, open an application and then click **Print**.

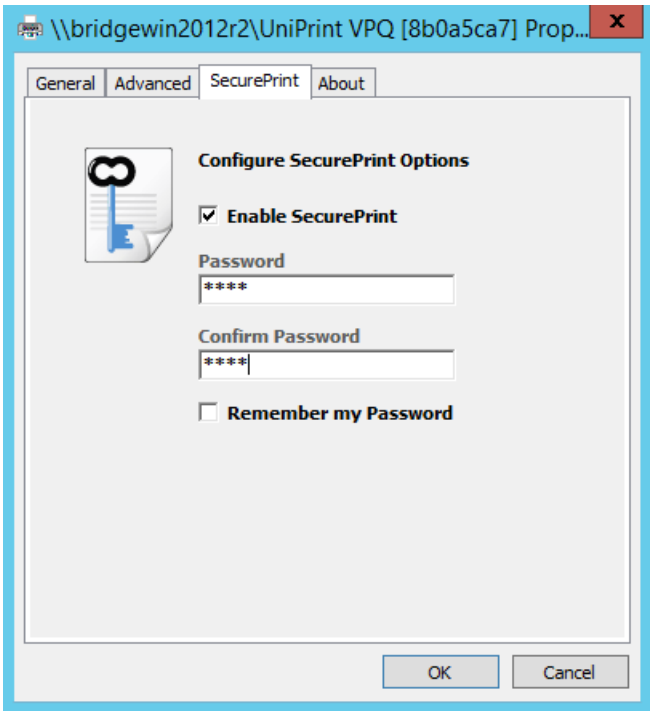
2. Select a Gateway printer or UniPrint VPQ and then click **Printer Properties**.



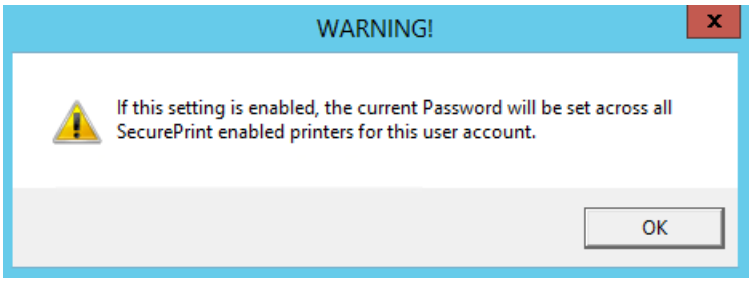
3. Click the **SecurePrint** tab.

4. Select **Enable SecurePrint.**

5. Enter your password twice. If you want your SecurePrint Password to remain persistent between sessions, select **Remember my Password**.



6. Click **OK** to clear the warning message and then click **OK** again.

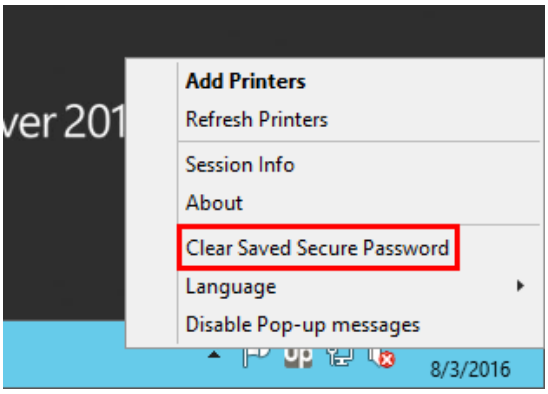


Resetting your SecurePrint Password

If **Remember my Password** was selected when you initially set your SecurePrint Password, you can clear the it by doing the following:

1. Within an RDP/ICA session, in the notification area, right-click .

2. Click **Clear Saved Secure Password**.



3. Click **Yes** to confirm that you want to reset your password.

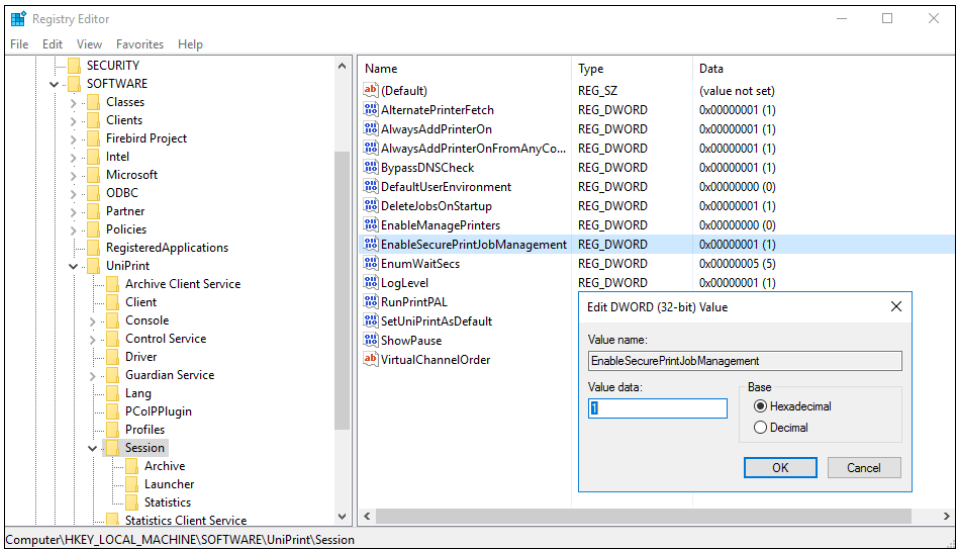
Managing the SecurePrint Queue Within a User's Session

If a user forgets their SecurePrint password, they can view and then delete a print job from within their RDP/ICA session.

To allow a user to manage their own SecurePrint queue, do the following:

1. On the Application Server, open the registry editor.

2. Under the following key, **HKEY_LOCAL_MACHINE\SOFTWARE\UniPrint\Session**, set **EnableSecurePrintJobManagement** to **1**.

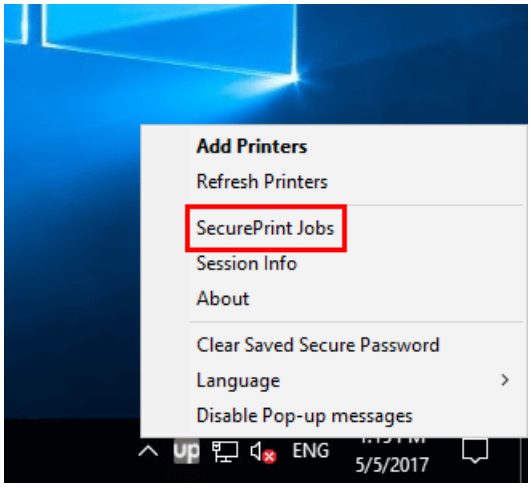


3. Close the registry editor.

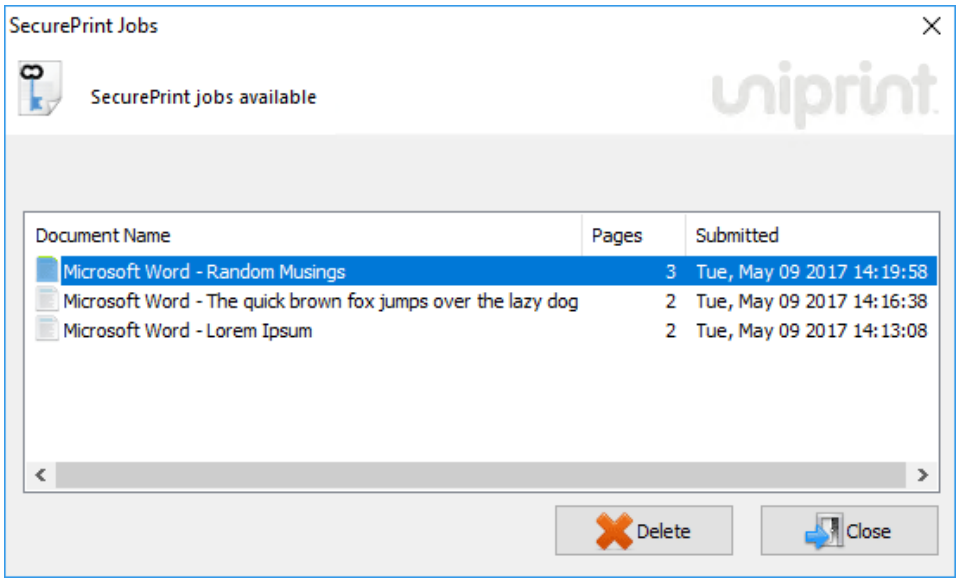
To delete a SecurePrint job within a user's session, do the following:

1. Within a user's session, in the notification area, right-click .

2. Click **SecurePrint Jobs**.



3. Click to select the print job to delete and then click **Delete**.



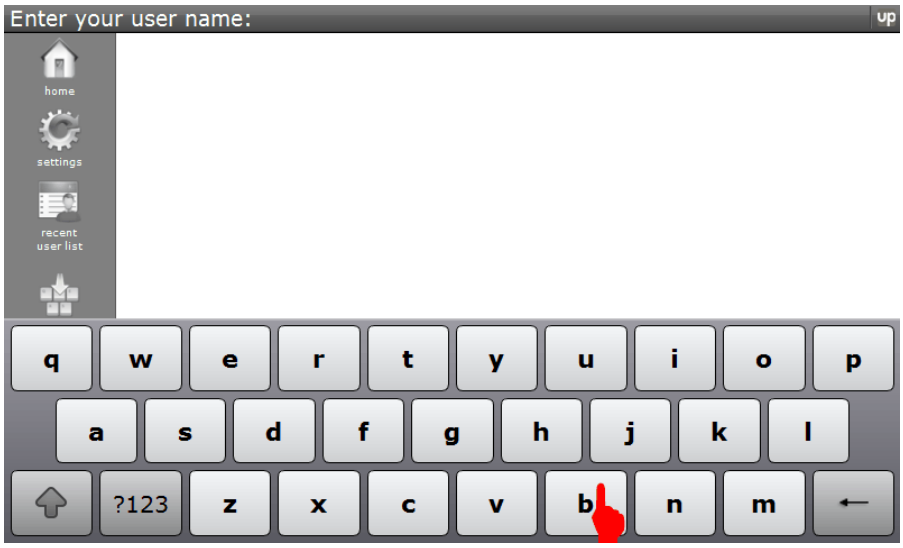
4. Click **Yes** to confirm that you want to delete the selected print job.

5. Click **Close**.

Retrieving Your Document Through the vPad Device

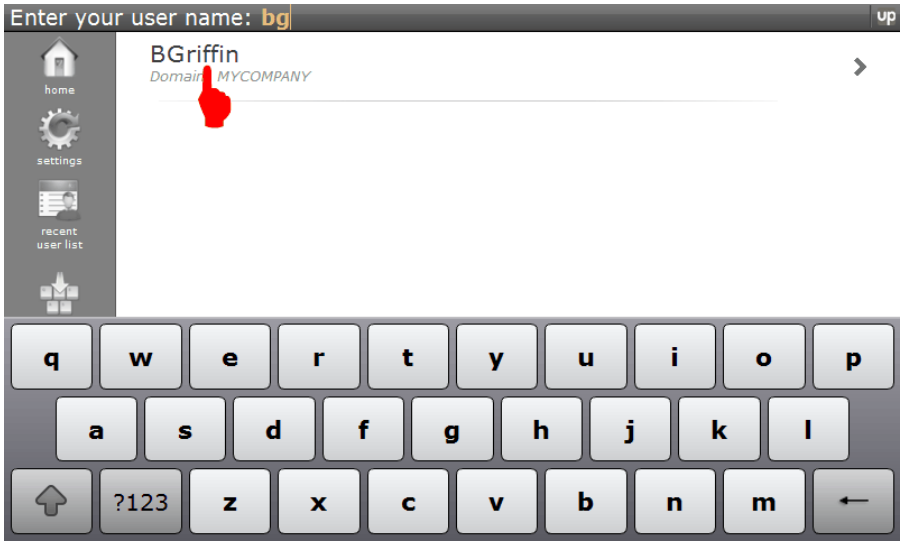
The following instructions assumes that a SecurePrint Password has been set.

1. At the vPad device, enter your user name using the keypad.

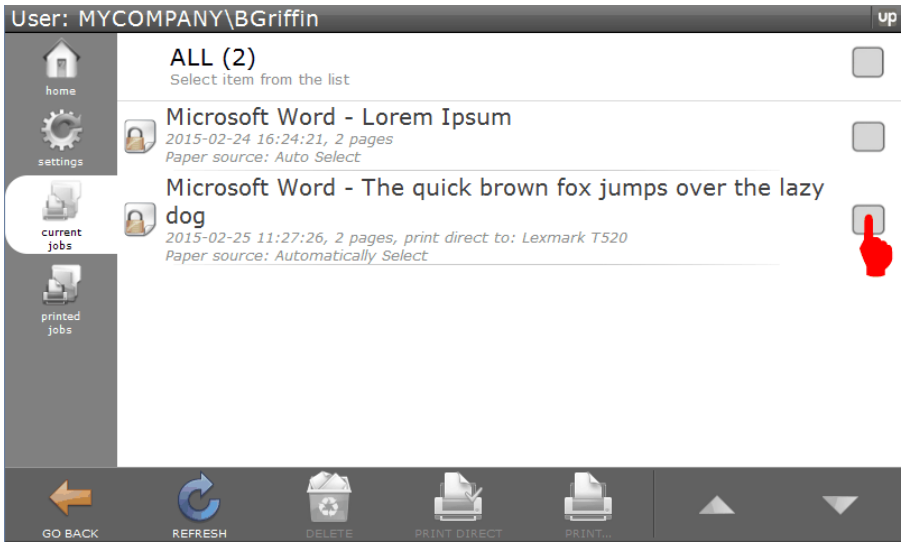


   a) Or tap **Hide Keypad**, .

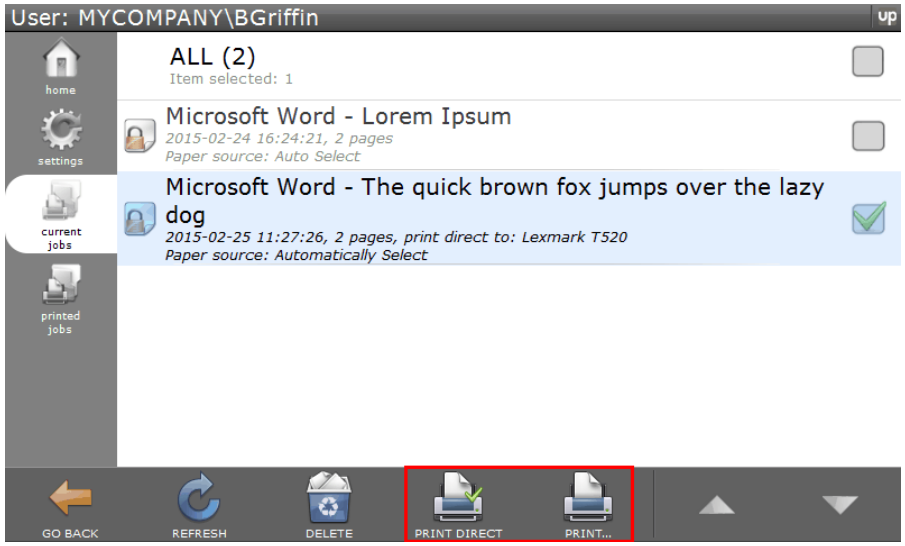
2. Tap your username.



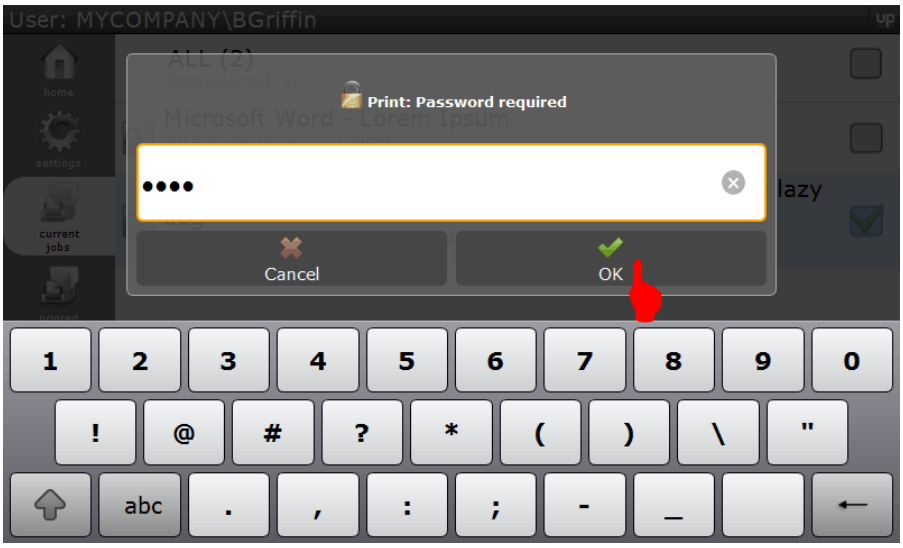
3. Tap to select the document that you want to print or tap **All** to print all documents associated with your user name.



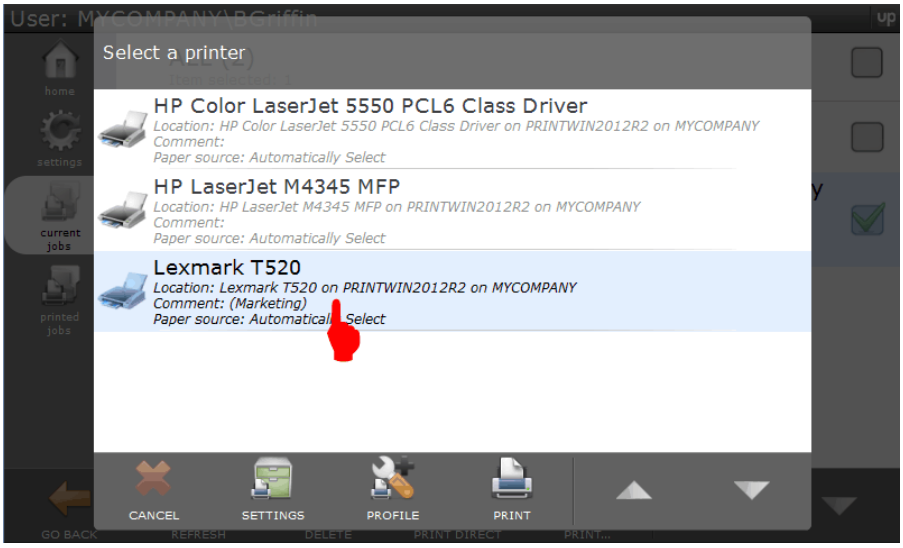
4. Tap either **Print** or **Print Direct**. If you print to a Gateway printer that is password protected, then you can avoid selecting a printer on the vPad by tapping **Print Direct**.



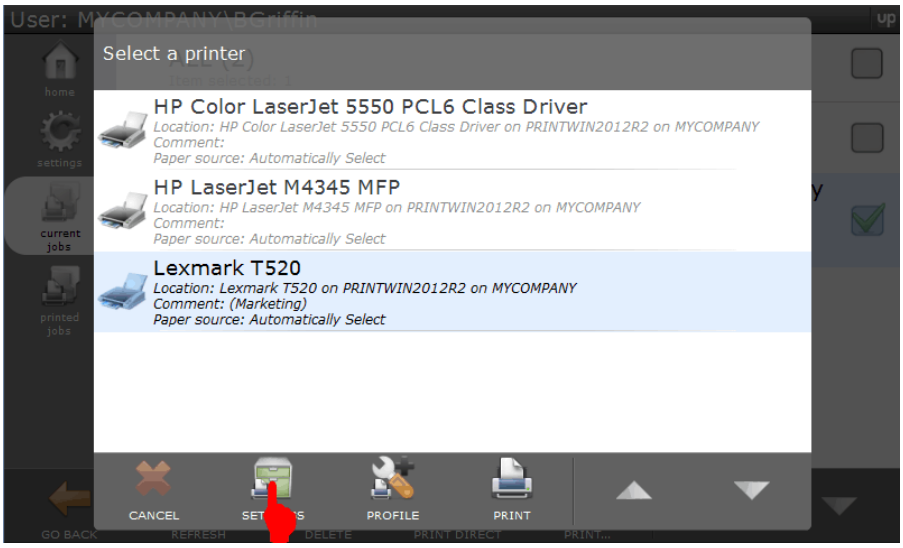
5. Enter your password and then tap **OK**.



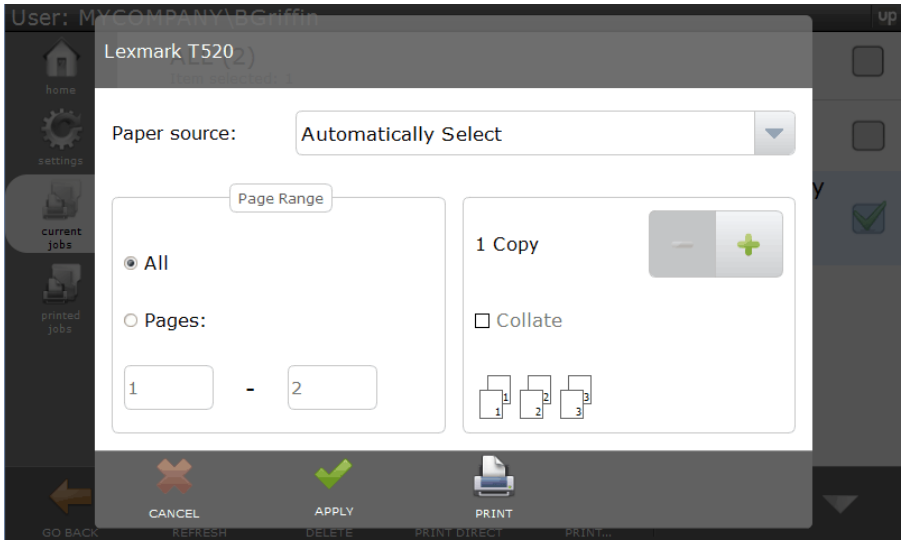
6. If you tapped **Print**, then tap to select a printer.



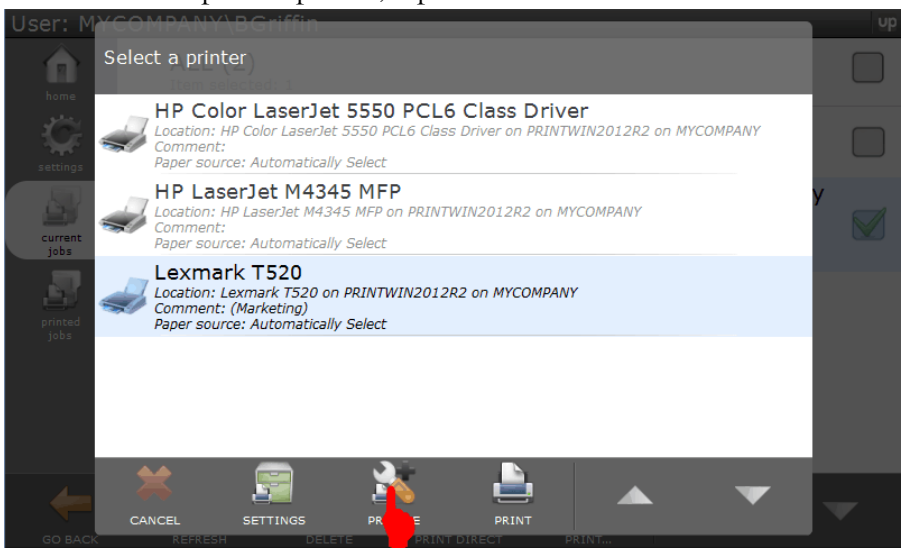
7. To change the paper source, page range or number of copies, tap **Settings**.



8. Tap to change the settings and then tap either **Apply**, if you have more settings to change, or tap **Print**, to print directly to the selected printer.

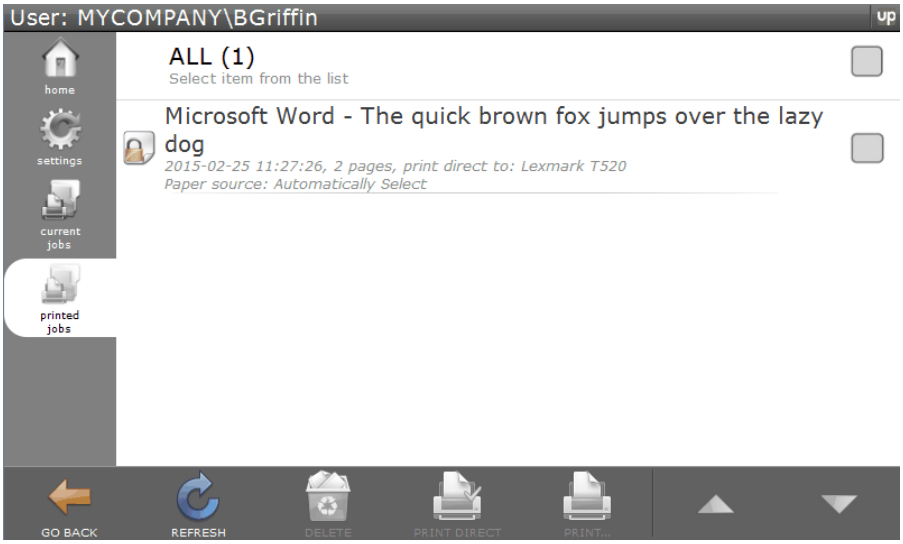


9. To select a printer profile, tap **Profile**.



10. Tap to select a profile and then tap either **Apply**, if you have more settings to change, or tap **Print** to print directly to the selected printer.

11. Tap **Print** and the print job will be released and sent to the selected printer with the specified printing preferences applied. The print job is also moved and can be accessed again from the **Printed Jobs** tab.



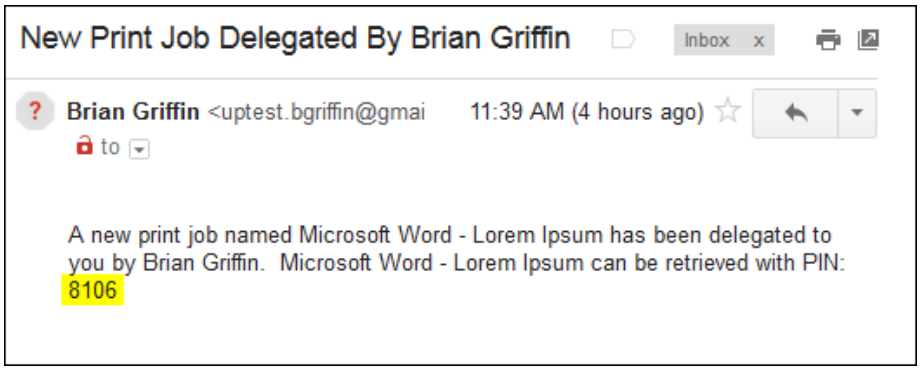
Retrieving a Delegated Print Job

After a print job has been delegated, the delegate receives an e-mail message with a 4-digit PIN that is to be used to release the print job to a printer.

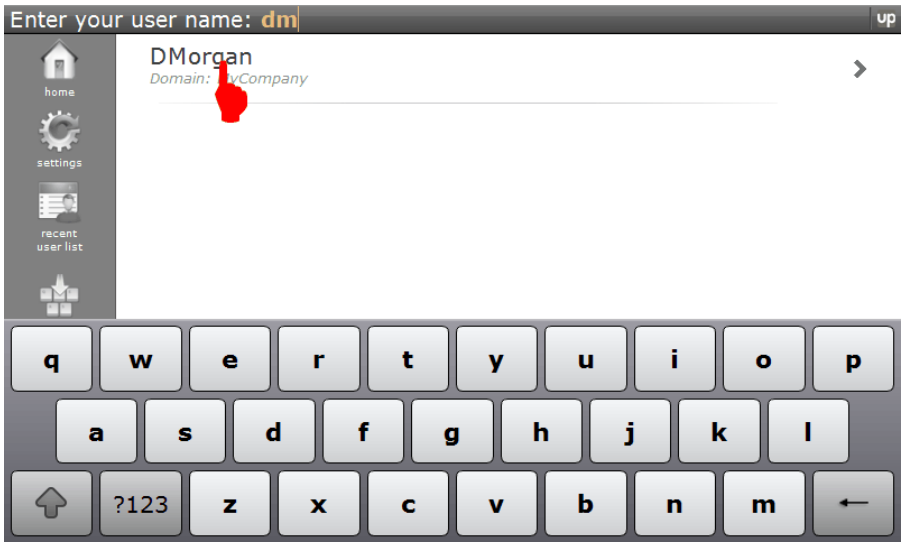
NOTE: Delegates who receive an e-mail message are only allowed to print the print job. They cannot delete the print job or alter the list of delegates.

To retrieve a delegated print job, do the following:

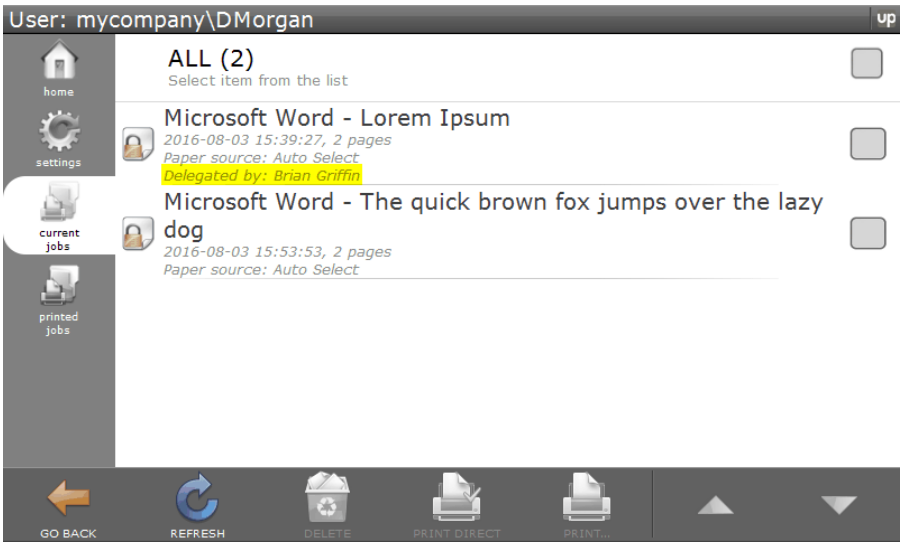
1. From the delegate print job e-mail message, remember the 4-digit PIN.



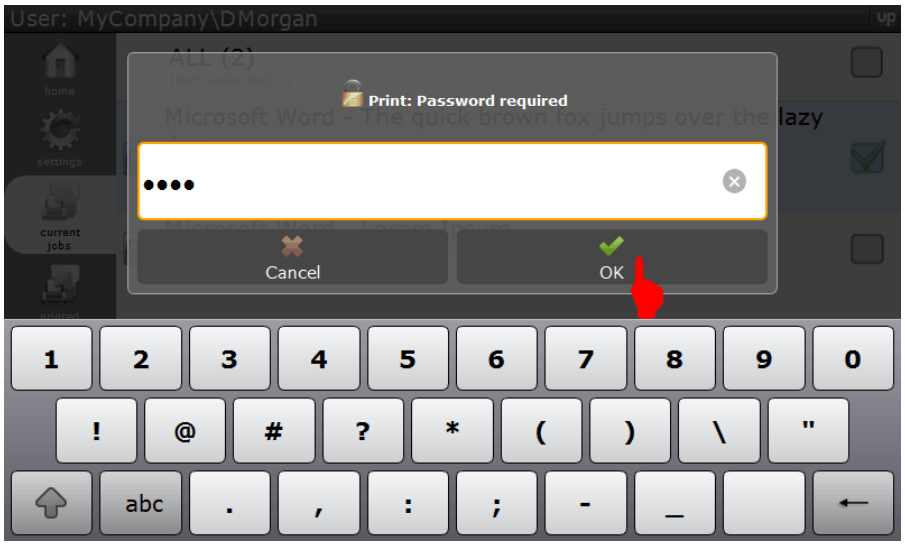
2. At the vPad device or emulator, enter your user name or use the arrows to locate your name. Tap to select your user name.



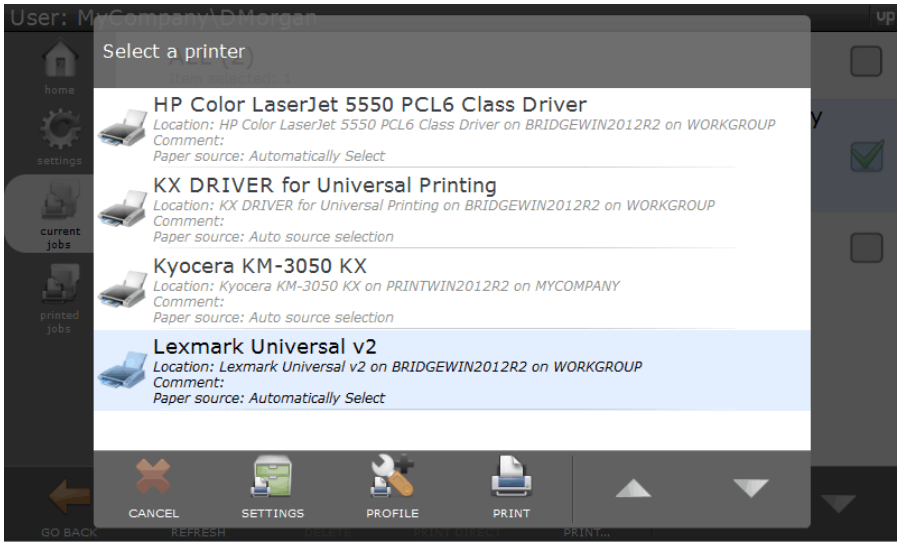
3. The print job will indicate who delegated the print job to you or the vPad. Tap to select the print job and then tap **Print**.



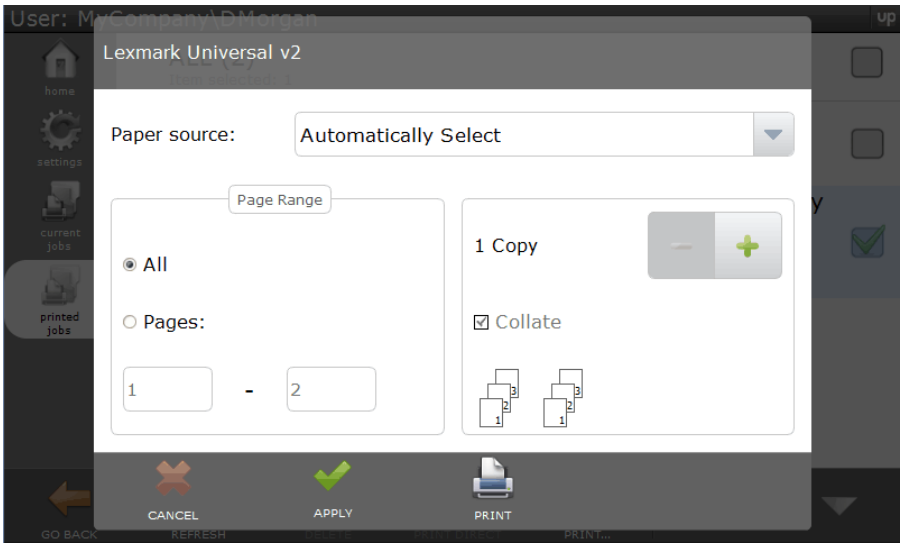
4. Enter the 4-digit PIN code from the e-mail you received and then tap **OK**.



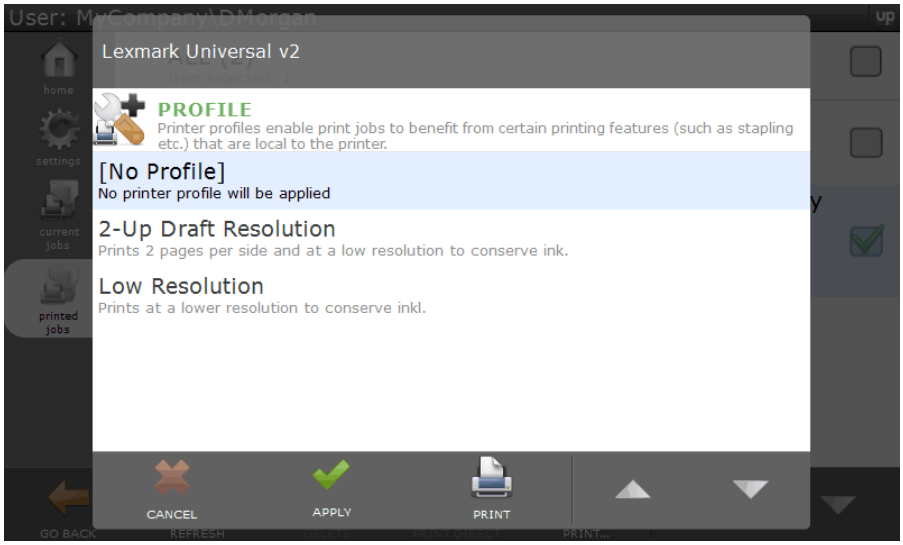
5. Tap to select a printer. To change printer settings, tap **Settings**. To select a printer profile, tap **Profile**.



a) Make changes to the printer settings and then tap **Apply**.

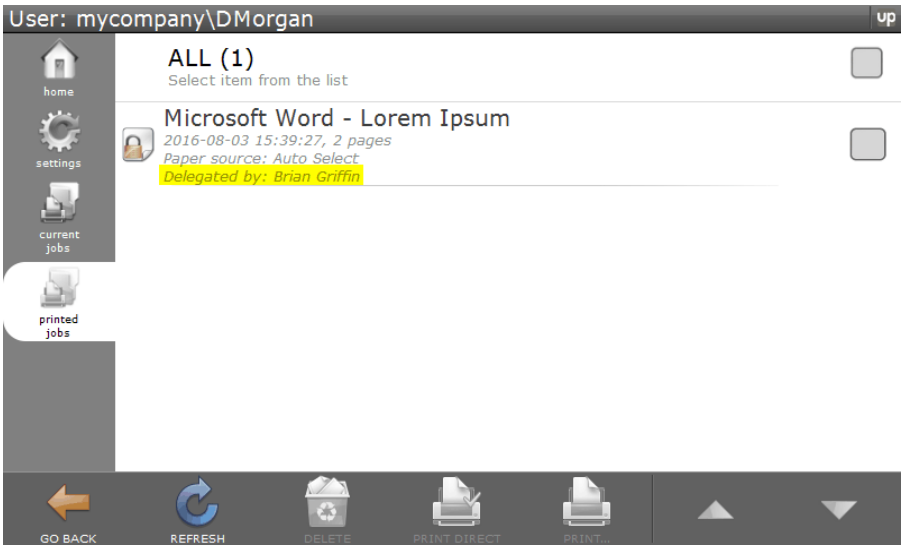


b) Tap to select a profile and then tap **Apply**.



6. Tap **Print** and the print job will print out at the selected printer.

7. The print job will then be deleted from the **Current Jobs** tab and placed in the **Printed Jobs** tab. This allows you to reprint if necessary.



CHAPTER 9

UniPrint Infinity

Configuring Print Job Archiving

Print Job Archiving allows network administrators to setup a location to archive all print jobs sent to any UniPrint Print Server or UniPrint Application Server that has the Archive Client installed.

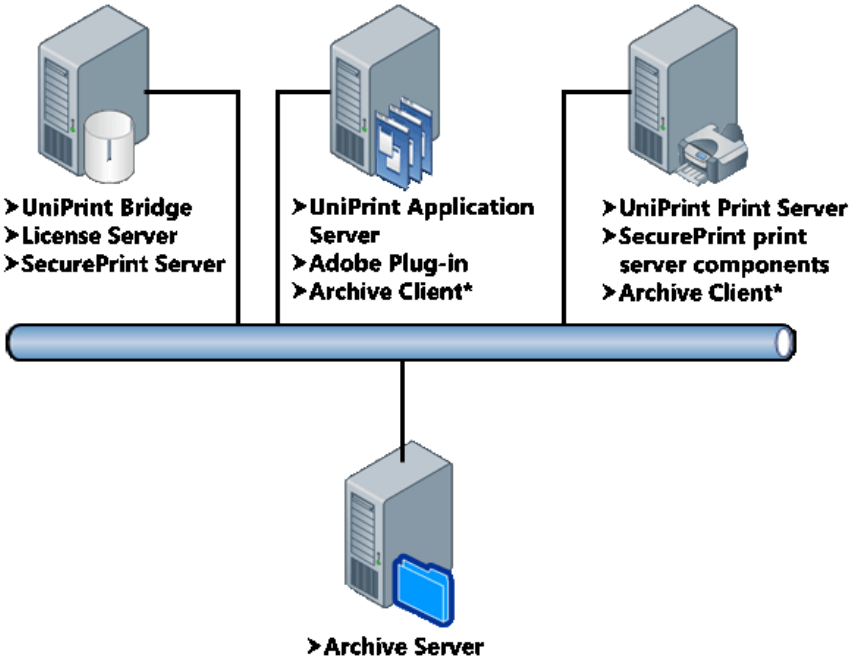
This feature differs from the UniPrint (Save PDF) queue in that the user does not have to actively select a print queue or change printer properties in order for their print job to be archived. The UniPrint (Save PDF) queue is intended to be used on a job-by-job basis, whereas Print Job Archiving will save a copy of all print jobs sent to the VPQ, Gateway printers, UniPrint queue, UniPrint (Email PDF) queue and UniPrint (Save PDF) queue.

Deployment Scenarios

The Archive Server can be installed on any Windows 2008/2012/2016 Server. By default, the location of the archive is where ever the Archive Server component is installed. Due to the sheer size of the print job archive, it is recommended that the Archive Server be installed on a separate, standalone server machine or device.

NOTE: Only one instance of the Archive Server can exist in a UniPrint deployment. While there can be many instances of the Archive Client depending on which print jobs are required for archiving.

Standard Deployment

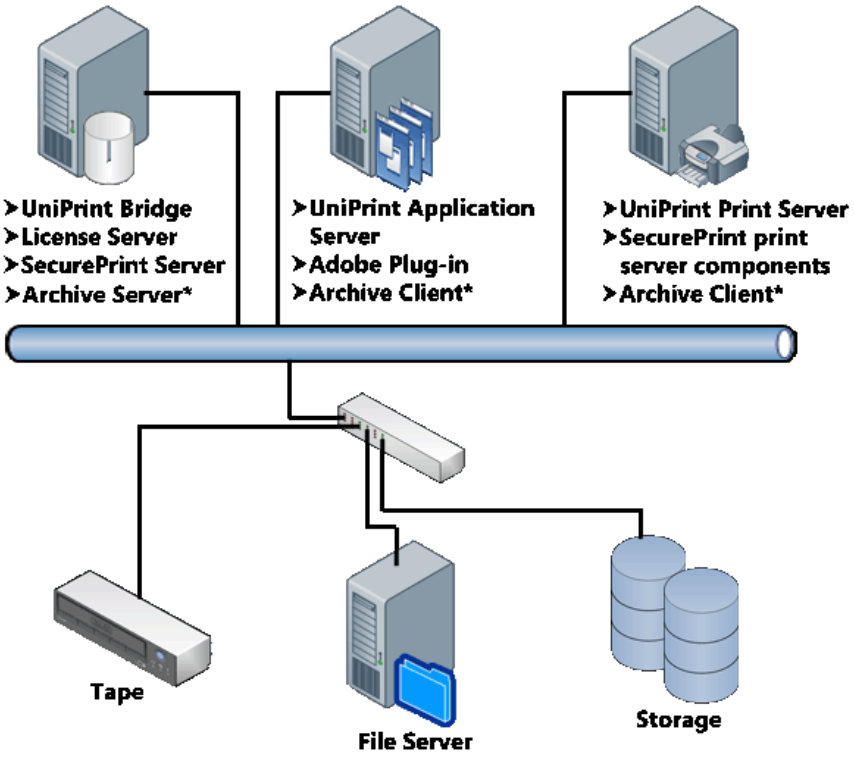


With the standard deployment, the Archive Server is installed on a separate, standalone machine. If the Archive Client is installed on the same machine as the UniPrint Application Server component, then all print jobs sent to the UniPrint queue and if enabled also to the UniPrint (Email PDF) and UniPrint (Save PDF) queues will be copied to the Archive Server. If the Archive Client is installed on the same machine as the UniPrint Print Server, then all print jobs sent to a Gateway printer queue will be copied to the Archive Server.

The default location is **//Program Files/UniPrint Suite/Services/Data/Archive**.

These archived files are saved as .PPF and .PCF files. The .PPF file is a copy of the actual PDF file and can be opened by changing the file extension to .PDF and opening it with a PDF reader. The .PCF file contains configuration information and PDF properties which can be read by opening the .PCF file with a text reader, such as Notepad.

Custom Deployment



In a custom deployment scenario, the Archive Server component can be installed on any of the other UniPrint components. In the example above, the Archive Server is installed on the UniPrint Bridge. From the UniPrint Bridge, the archiving can be redirected to a network location as long as the system account rights are the same in both locations – the Archive Server location and the mapped drive location.

BEST PRACTICE: It is recommended that the Archive Server component be installed on the same computer where the print jobs are to be archived. See "Standard Deployment" on page 320.

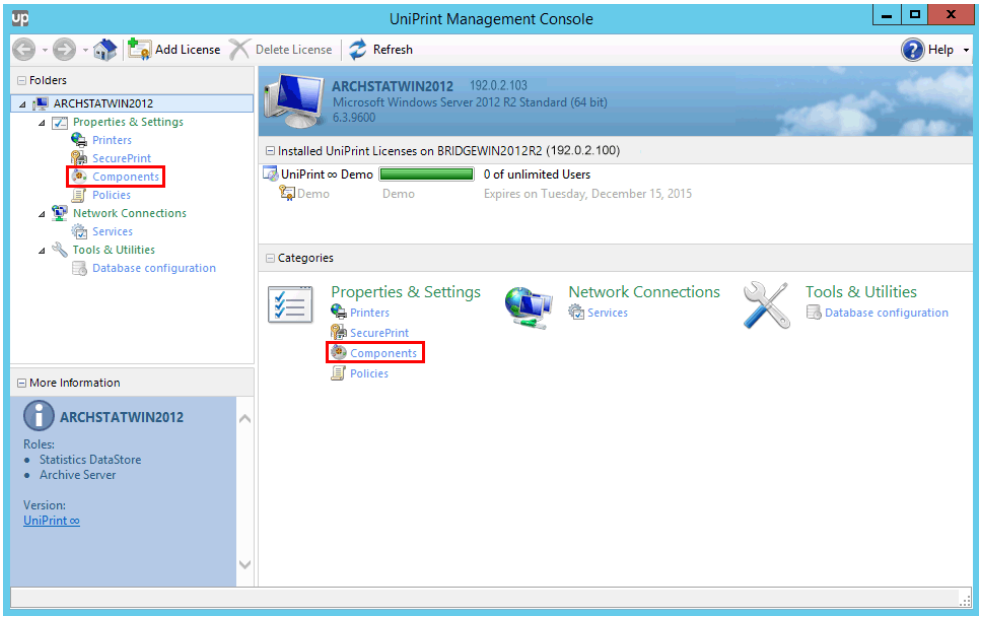
UniPrint printer print jobs are archived, if the Archive Client is installed on the UniPrint Application Server and Gateway printer print jobs are archived, if the Archive Client is installed on the UniPrint Print Server.

Changing the Archive Location

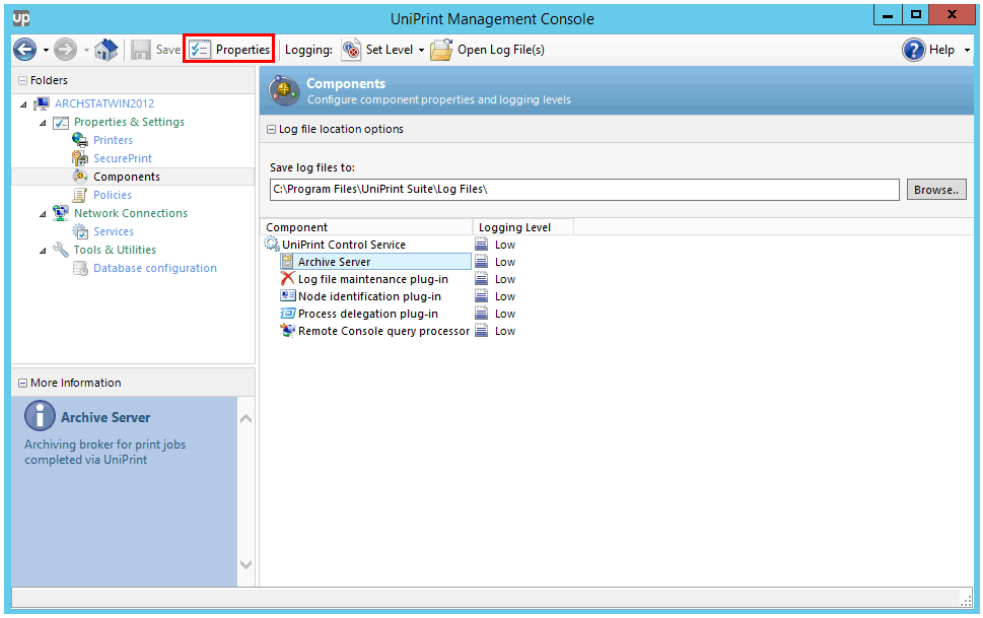
By default print jobs are archived on the Archive Server. However, the location can be changed by doing the following:

1. On the Archive Server, open the **UniPrint Management Console**.

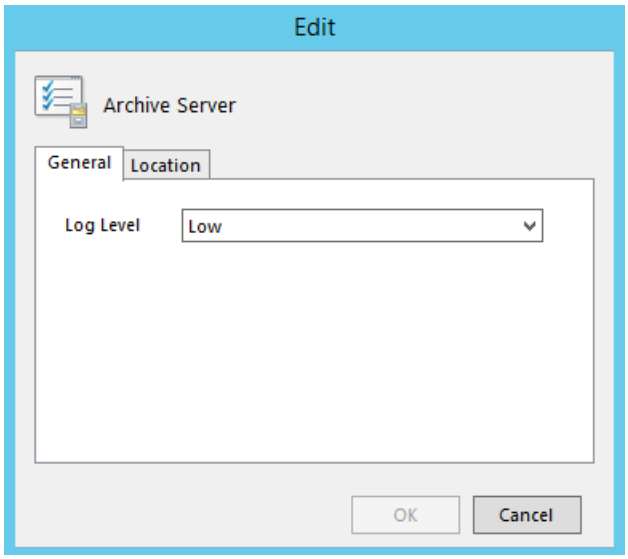
2. Under **Properties & Settings**, click **Components**.



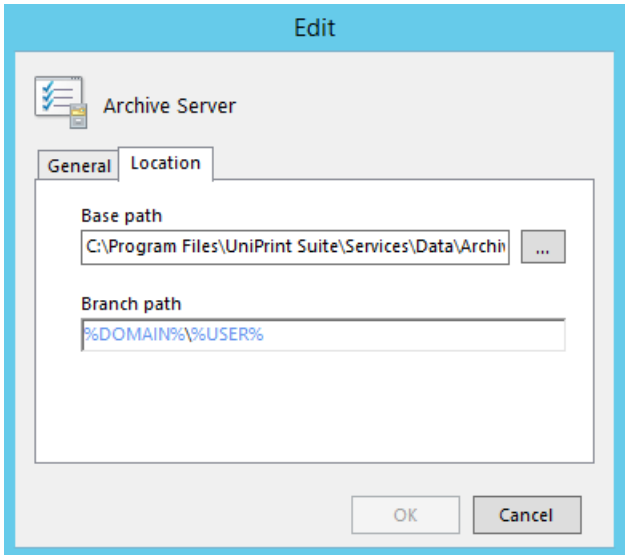
3. Click to select **Archive Server** and then click **Properties**.



4. Click the **Location** tab.



5. Click ... and then browse to a new location.



6. Click **OK** and then click **OK** again.

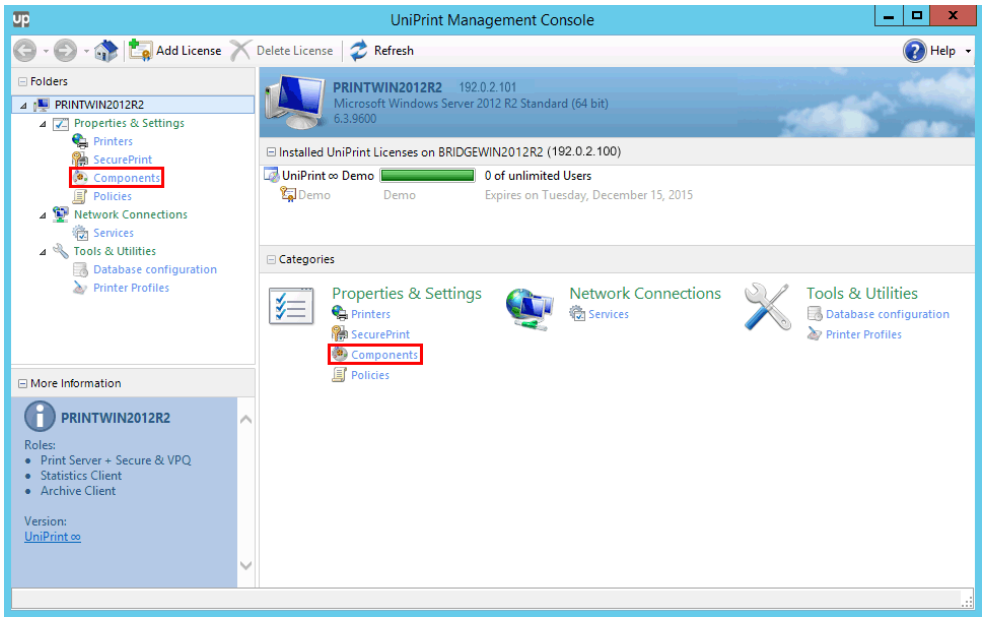
Restricting When Print Jobs Are Archived

Print job archiving can be restricted to occur during a certain time of the day. For example, if print jobs are only to be archived during business hours, then the time frame can be set.

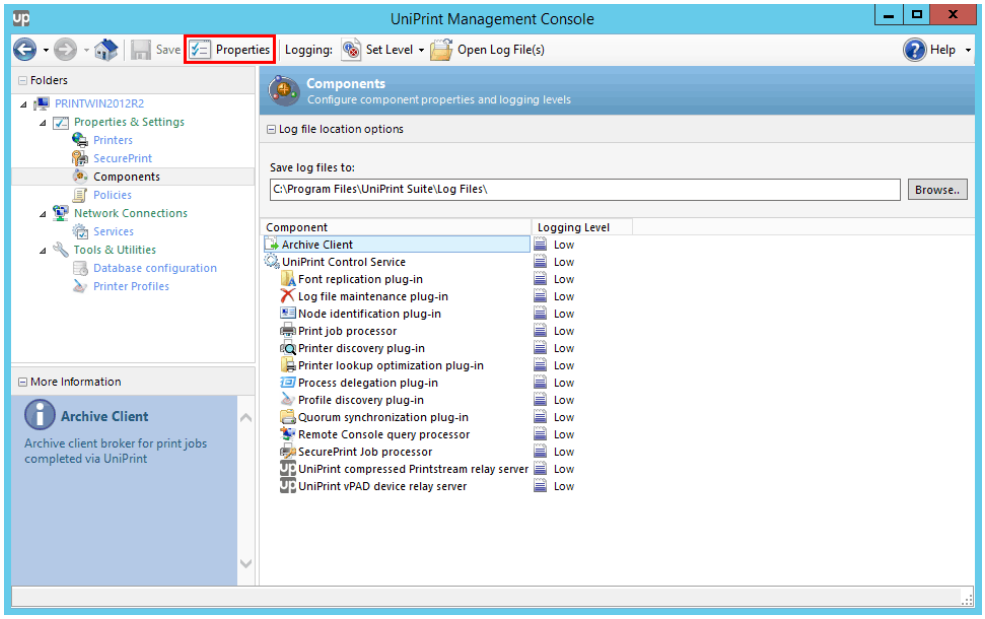
To restrict when print jobs are archived, do the following:

1. On the either the UniPrint Application Server or UniPrint Print Server, open the **UniPrint Management Console**.

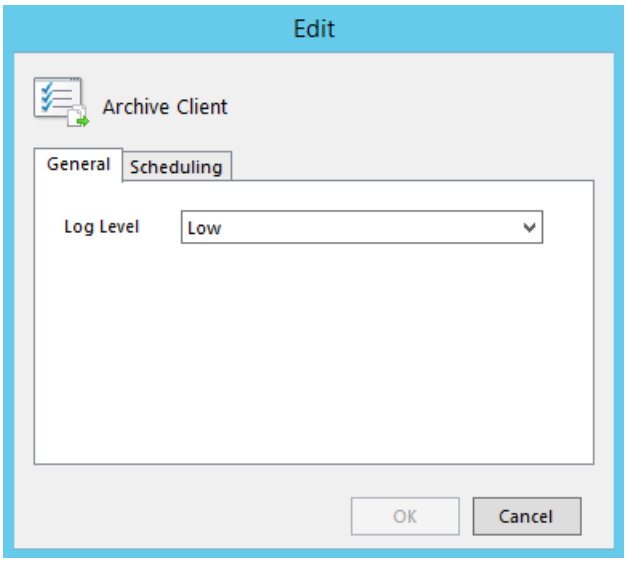
2. Under **Properties & Settings**, click **Components**.



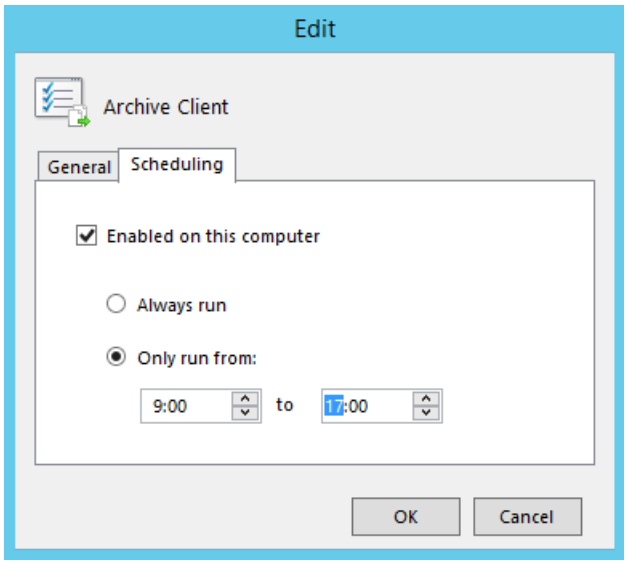
3. Click to select **Archive Client** and then click **Properties**.



4. Click the **Scheduling** tab.



5. Select **Only run from** and then edit the time to run print job archiving. Click **OK**.



CHAPTER 10

UniPrint Infinity

Retrieving Print Job Statistics

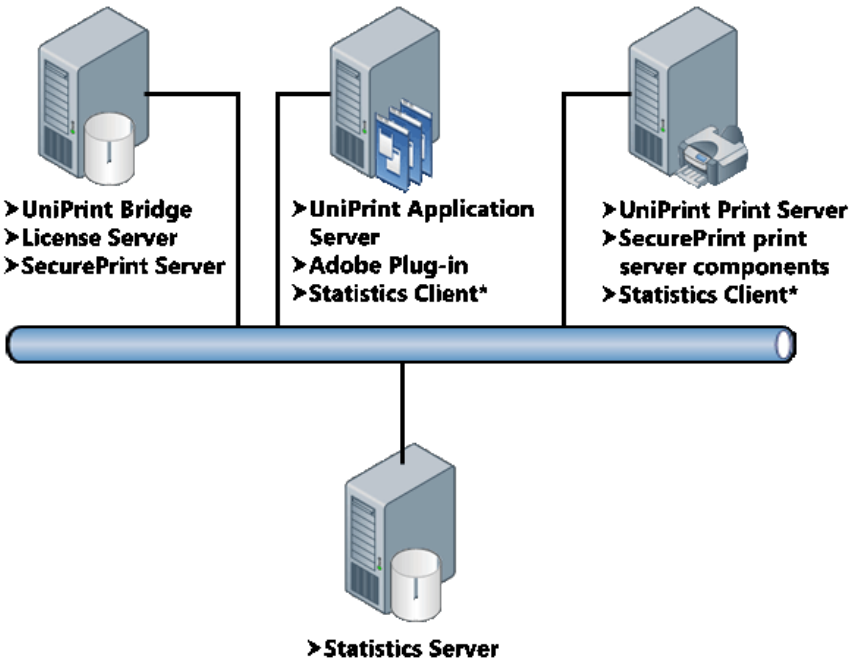
Print Job Statistics Monitoring allows network administrators to capture print job statistics from printers installed on any UniPrint Print Server or from the UniPrint, UniPrint (Save PDF) and UniPrint (Email PDF) print queues on the UniPrint Application Server that has the Statistics Client installed.

Deployment Scenario

The Statistics Server can be installed on any Windows 2008/2012/2016 server. Due to the amount of data collected, it is recommended that the Statistics Server component be installed on an independent, standalone, server class machine. By default, the location of the statistics database is where ever the Statistics Server component is installed.

NOTE: Only one instance of the Statistics Server can exist in a UniPrint deployment. While there can be many instances of the Statistics Client depending on which print jobs require monitoring.

Standard Deployment



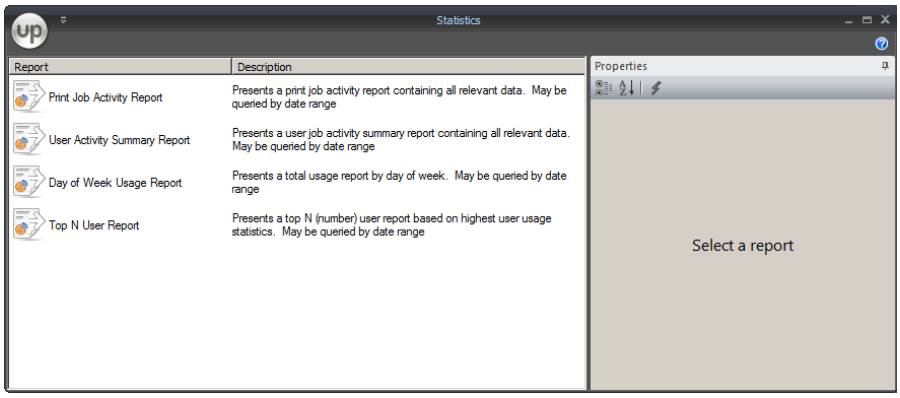
With the standard deployment, the Statistics Server is installed on a separate machine. If the Statistics Client is installed on the same machine as the UniPrint Application Server component, then all print job statistics will be captured from the UniPrint queue and if enabled also to the UniPrint (Email PDF) and UniPrint (Save PDF) queues and then stored on the Statistics Server. If the Statistics Client is installed on the same machine as the UniPrint Print Server, then all print job statistics will be captured from all Gateway printer queues and stored on the Statistics Server.

Retrieving Print Job Data From The Statistics Server

Statistics can be retrieved and displayed from any application that can establish an ODBC connection to the statistics database. The following steps demonstrate how to do this using Microsoft Access 2016. For other

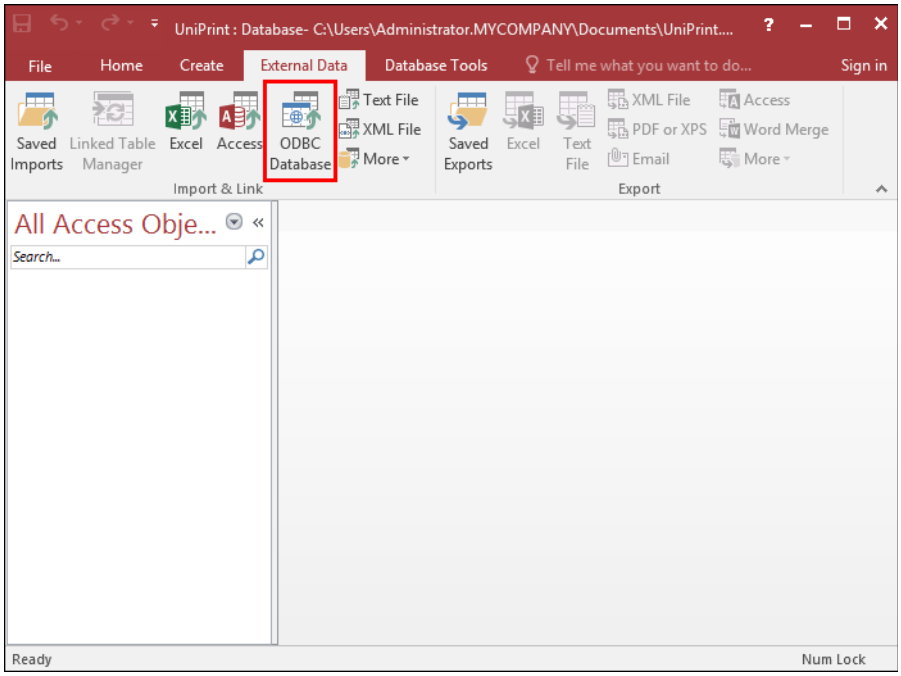
applications, for example Crystal Reports, refer to the product documentation on establishing an ODBC connection and importing a database.

NOTE: The UniPrint Statistics Viewer is also available and can be downloaded from https://uniprint.net/eng/page/download-tools-and-utilities. *.NET Framework 3.5 must be installed prior to installing the UniPrint Statistics Viewer.*

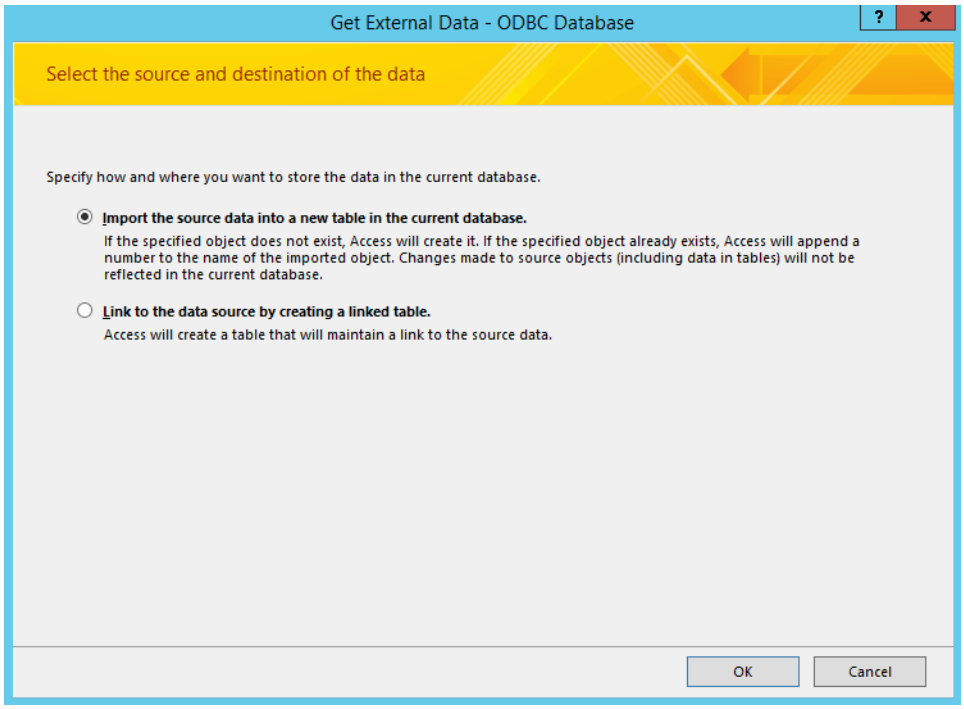


1. On the Statistics Server, open Microsoft Access.

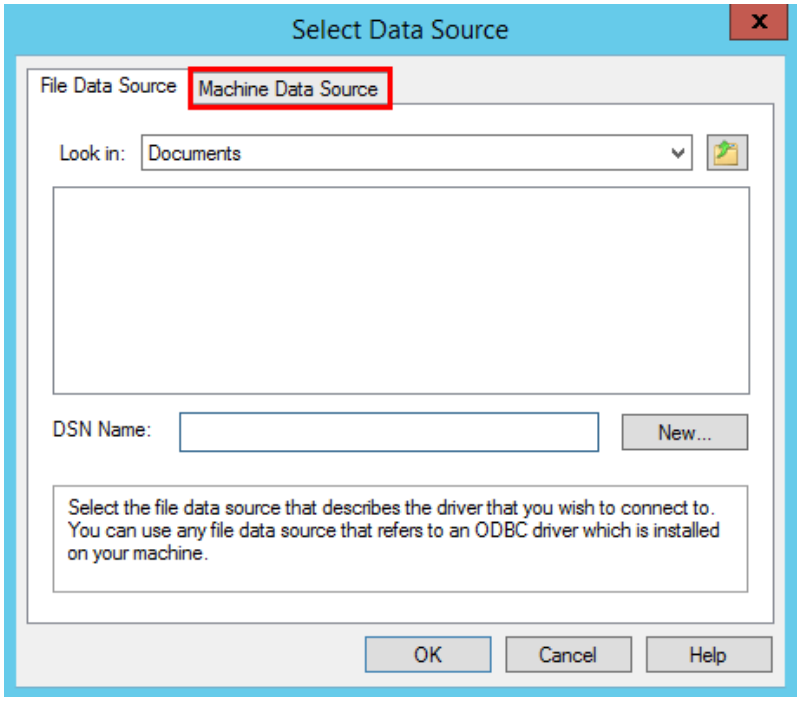
2. Click the **External Data** tab and then click **ODBC Database**.



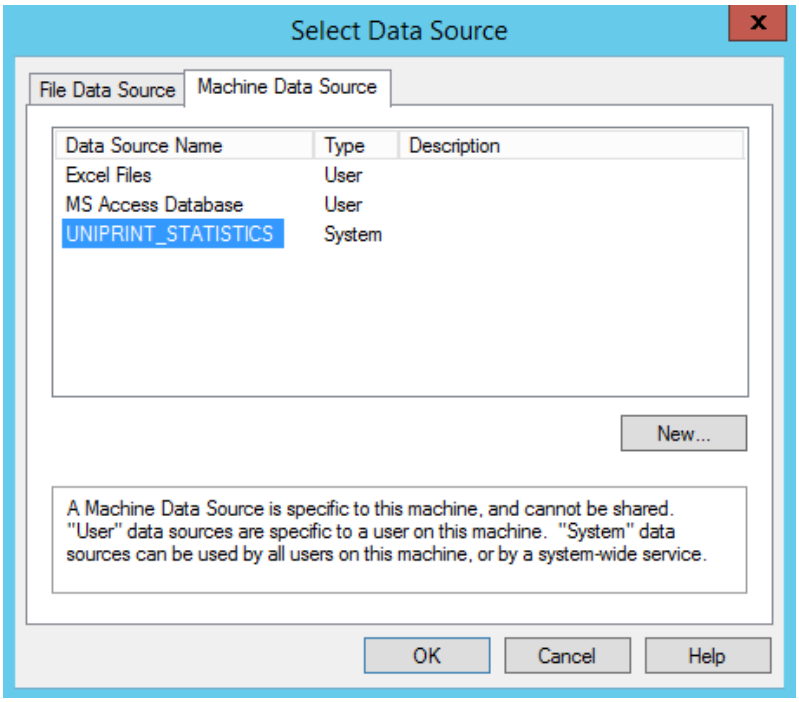
3. Select **Import the source data into a new table in the current database** and then **click OK**.



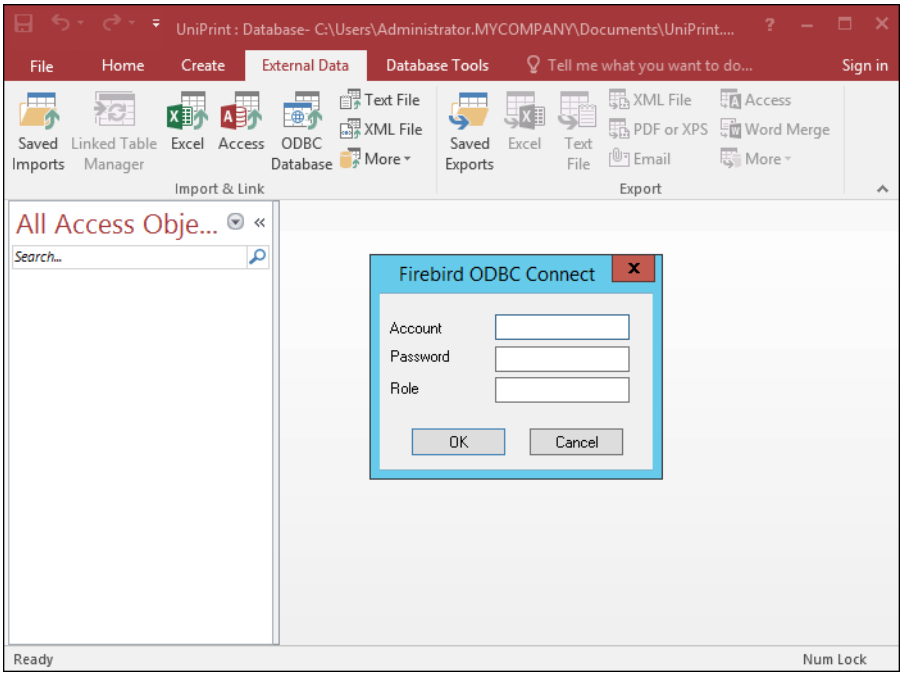
4. Click the **Machine Data Source** tab.



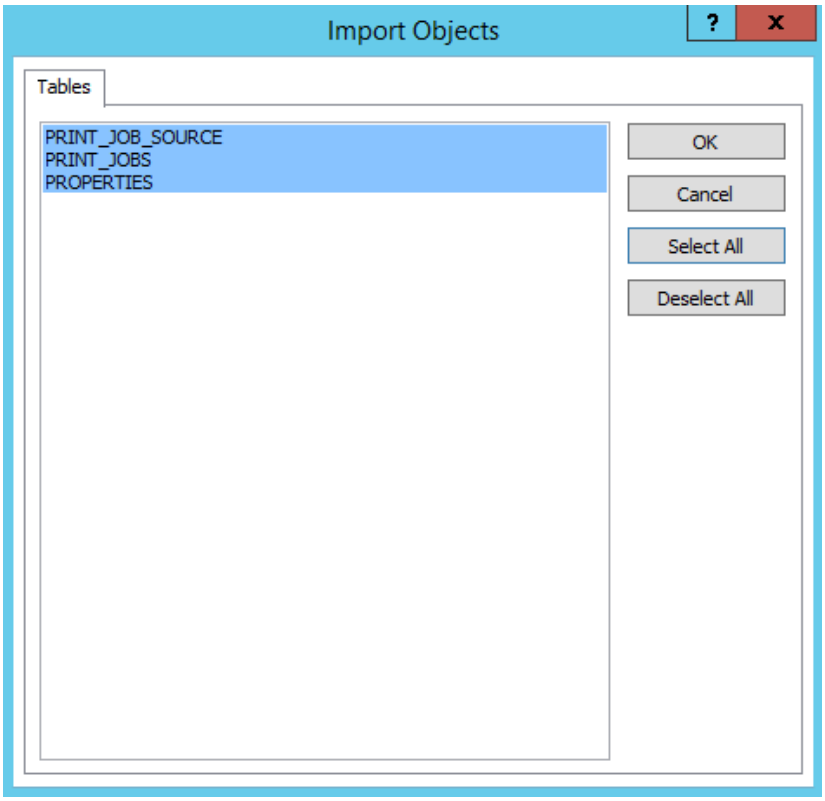
5. Click to select **UNIPRINT_STATISTICS** and then click **OK**.



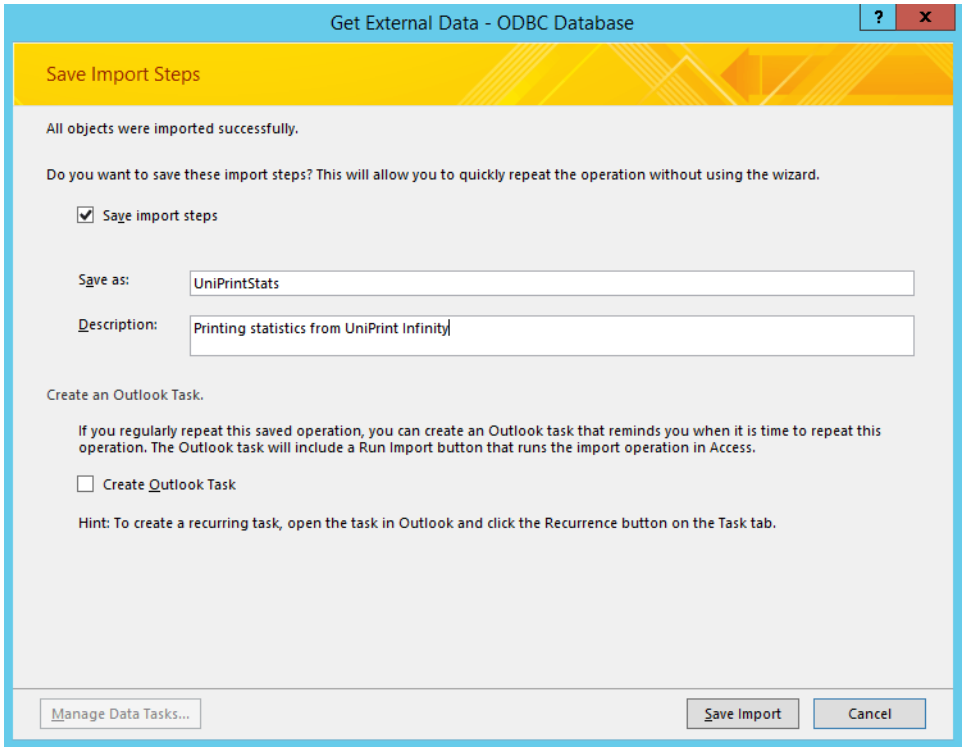
6. Enter the default credentials and then click **OK**. Contact UniPrint Support for database access information.



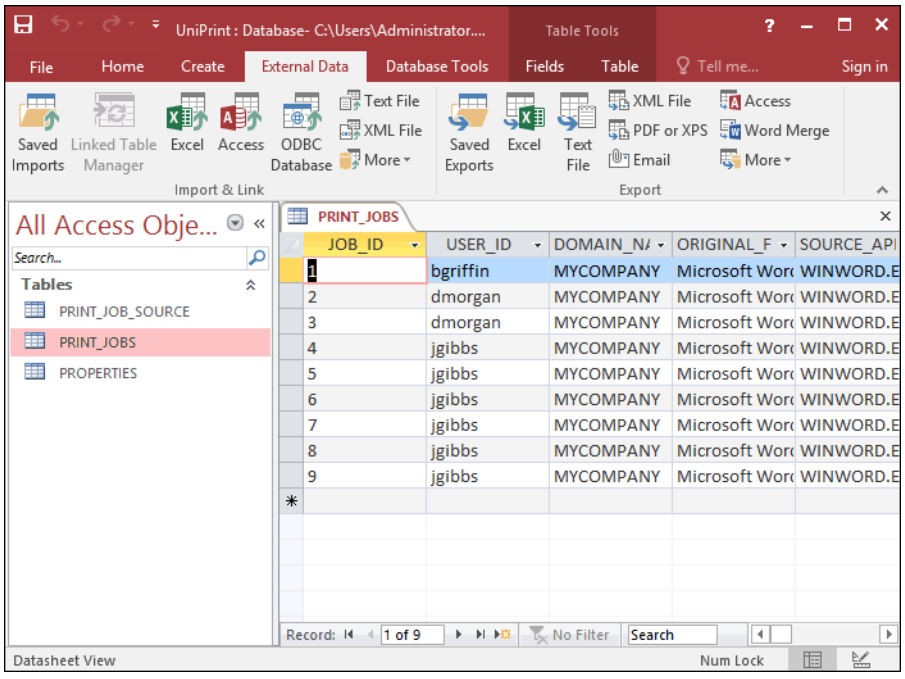
7. Click **Select All** and then click **OK**.



8. To make retrieving data faster the next time it is required, select **Save import steps** and then give it a name and a description. Click **Save Import**.



9. Double-click **PRINT_JOBS** to view the data collected.



CHAPTER 11

UniPrint Infinity

Printing with UniPrint Infinity

This chapters covers how to print from within a user's RDP or ICA session using UniPrint Infinity and its features, with the exception of the UniPrint One Queue where printing can be done outside of a user's session.

The following instruction set is based on a Windows Server 2012 R2 session. For other operating systems, refer to its documentation to make the appropriate adjustments.

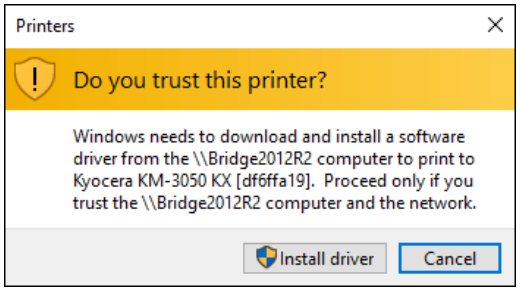
Adding a UniPrint Gateway Printer

After a printer is added on the UniPrint Print Server and then published to the UniPrint Bridge, it becomes a UniPrint Gateway printer.

There are three ways to add a Gateway printer:

- In their session, the user can add it manually in a session.
- If PrintPAL has been configured to the run on the Application Server, the user can add a Gateway printer through the UniPrint icon in the notification area.
- Through the UniPrint One Queue which allows guest users to add a Gateway printer without having to login or install the UniPrint Application Server on their machines.

NOTE: If the UniPrint Bridge and the UniPrint Application Server are located in different time zones, the user maybe prompted to install the driver.



This is a Windows function and is due to the drivers on the UniPrint Bridge having a different timestamp from that of the drivers on the UniPrint Application Server.

Adding a Gateway Printer Manually

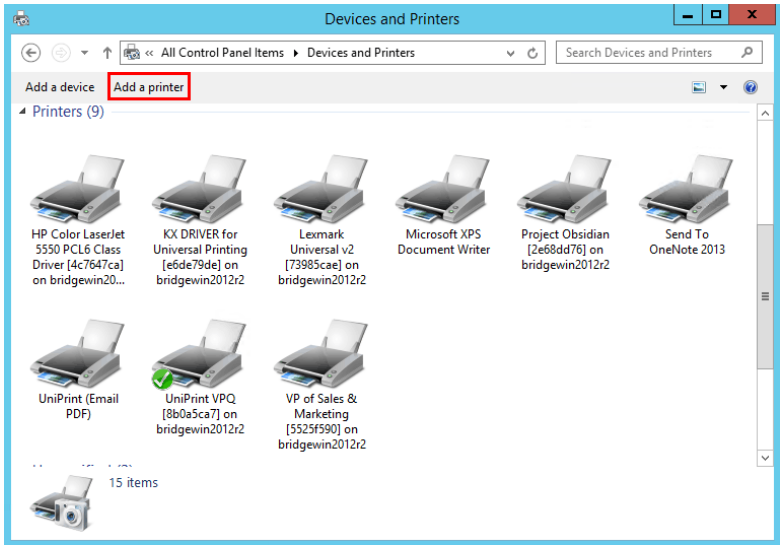
In order for the user to print to a Gateway printer, they first need to add it in their session. To alleviate this process for the user, you can always use PrintPAL to automatically add printers on their behalf.

To add a Gateway printer from within a user's session, do the following:

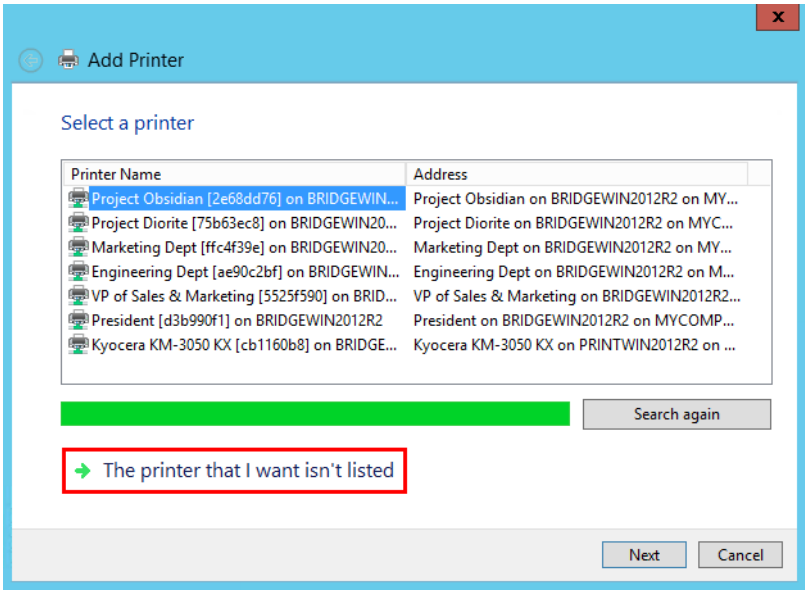
1. Log onto the Application Server as you normally would through RDP or ICA to access applications.

2. Click **Start**, click **Control Panel** and then click **Devices and Printers**.

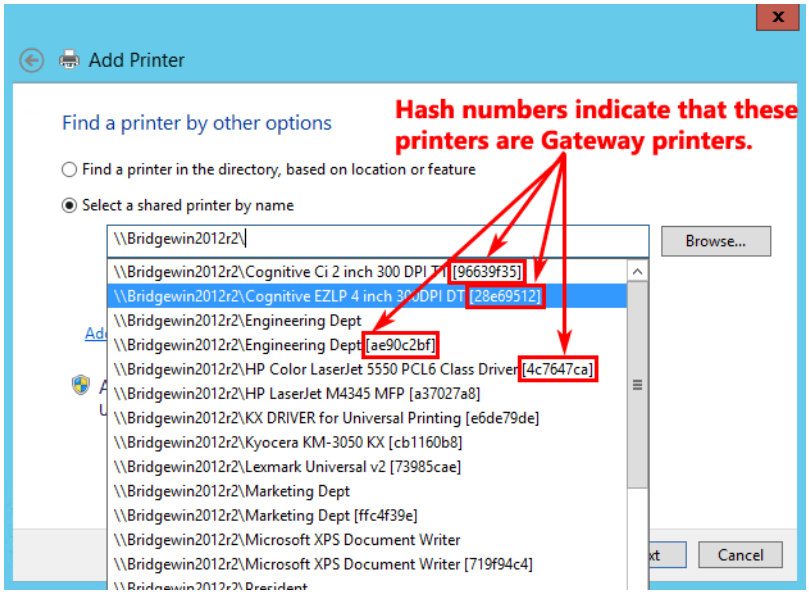
3. Click **Add a printer**.



4. Click to select a Gateway printer which are usually indicated with hash numbers. If the printer that you want doesn't appear in the list, click **The printer that I want isn't listed**.

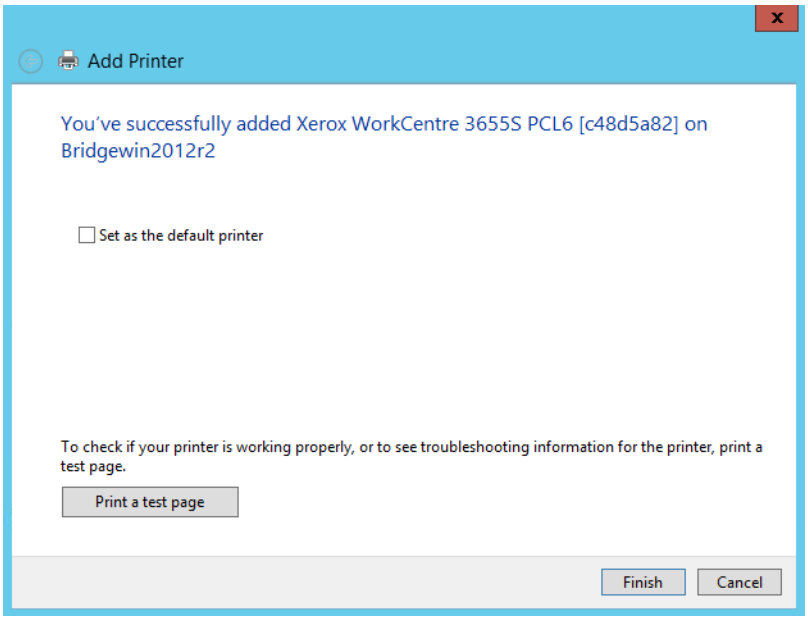


5. Type \\[***BridgeHostName***]\, click to select a Gateway printer and then click **Next**. Hash numbers are used to ensure that each Gateway printer is unique and for users they are good indicators that the printer is indeed a Gateway printer.

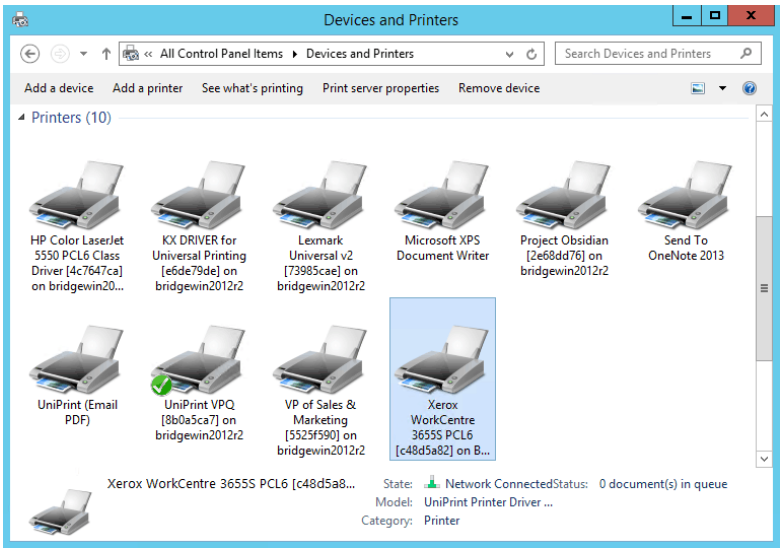


6. Click **Next**.

7. If you want this printer to be set as the session default, select **Set as default printer** and then click **Finish**.



The Gateway printer is now added to the session and is available for printing.



Adding a Gateway Printer Using PrintPAL And UPSession

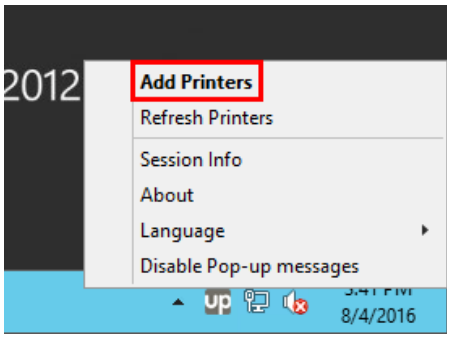
Once PrintPAL has been configured, PrintPAL will automatically map printers to the user's session. However, if the user wants to add an additional printer they can do so through UPSession which is represented by the UniPrint icon in the notification area.

To add a Gateway printer through PrintPAL and UPSession, do the following:

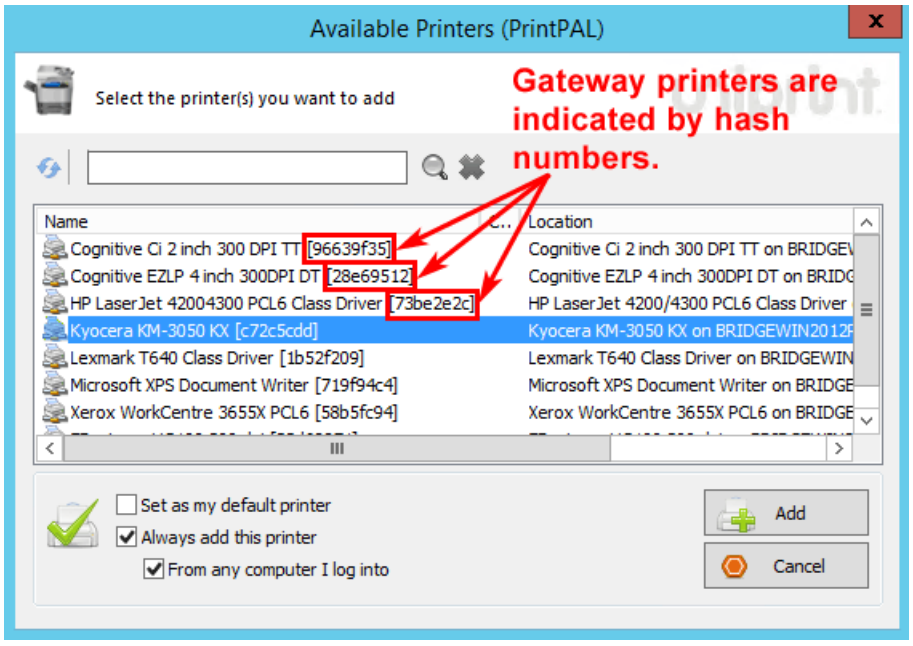
1. Log onto the application server as you normally would through RDP or ICA to access applications.

2. In the notification area, right-click .

3. Click **Add Printers**.

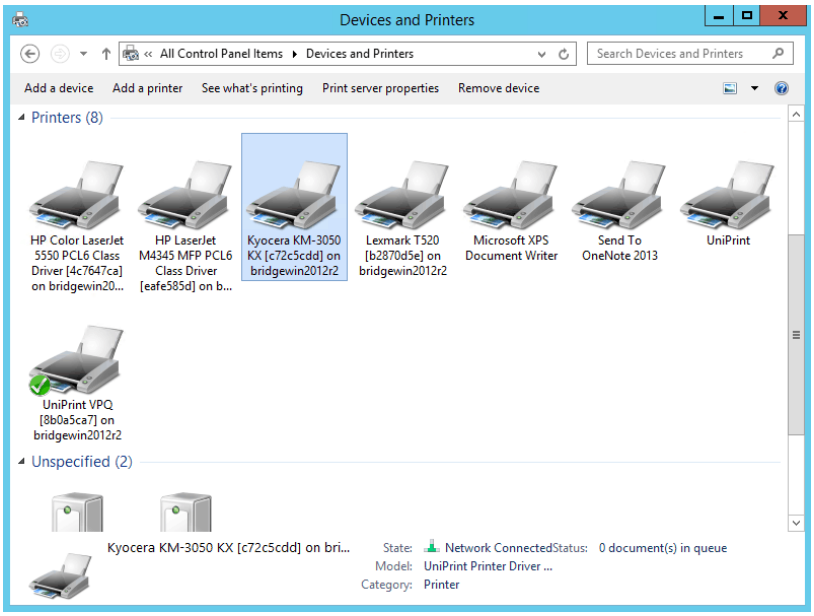


4. Click to select a Gateway printer which are usually indicated with hash numbers. To make this printer the default, click **Set as my default**. To ensure this printer is always added, even after the user logs out and then back in again, click **Always add this printer**. To ensure this printer is always added, no matter which device the user logs in from, click **From any computer I log into**.



5. Click **Add**.

6. The selected Gateway printer will be added to the user's session.



Adding a Gateway Printer Using the One Queue (Session Login Not Required)

The UniPrint One Queue can be used by guest users to print to a Gateway printer without being required to log into an ICA/RDP session or install UniPrint Application Server on their local machines. A Gateway printer is simply added to the guest machine and the UniPrint core components are also installed that allows the user to print to this printer and use any features such as printer profiles that maybe associated with this Gateway printer. If the Gateway printer is removed, the UniPrint core components are also removed from the device.

NOTE: Since the UniPrint One Queue was designed and is intended for guest printing only, PrintPAL cannot be used to add additional printers. If PrintPAL is to be used, the full Application Server component is required on the guest machine.

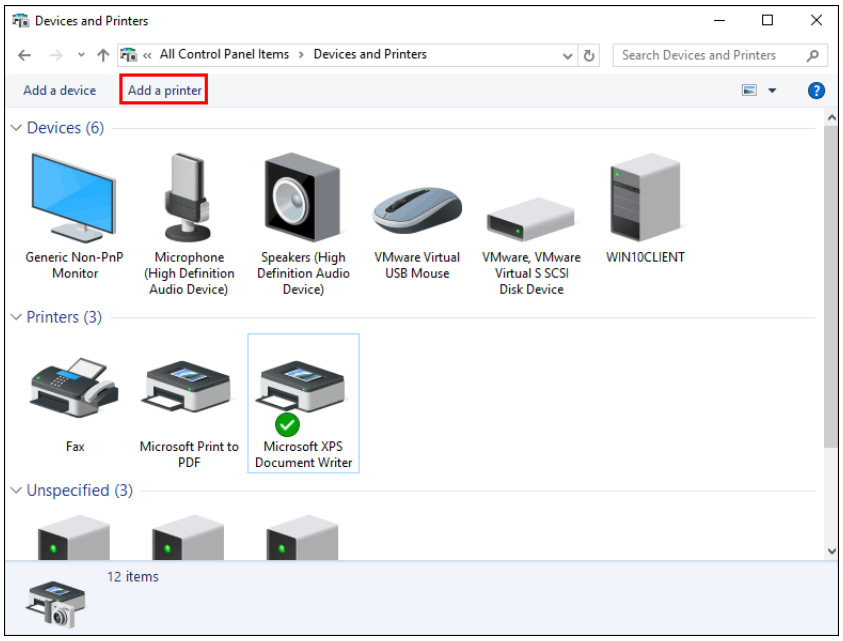
The following instructions are based on Windows 10. For other operating systems, refer to the documentation for that operating system to make the appropriate adjustments.

To add a Gateway printer, do the following:

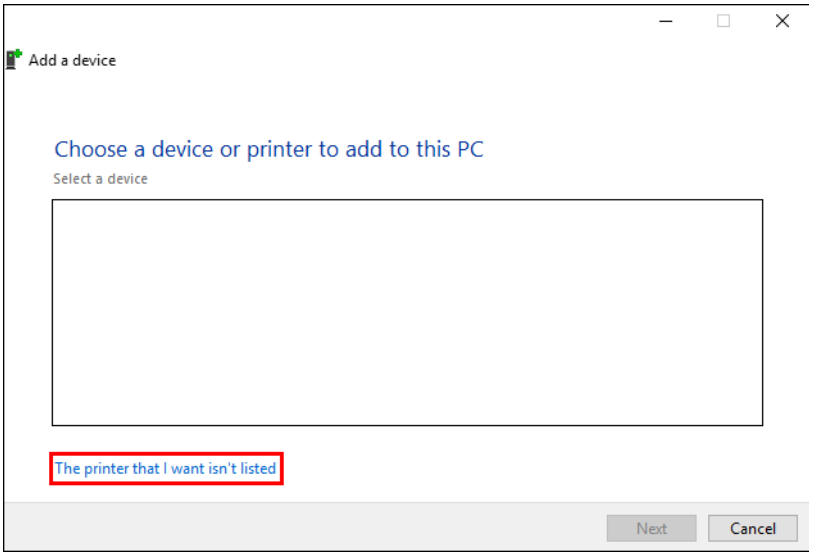
1. Click **Start** and then type `Control Panel`.

2. Click **Control Panel** and then click **Devices and Printers**.

3. Click **Add a printer**.

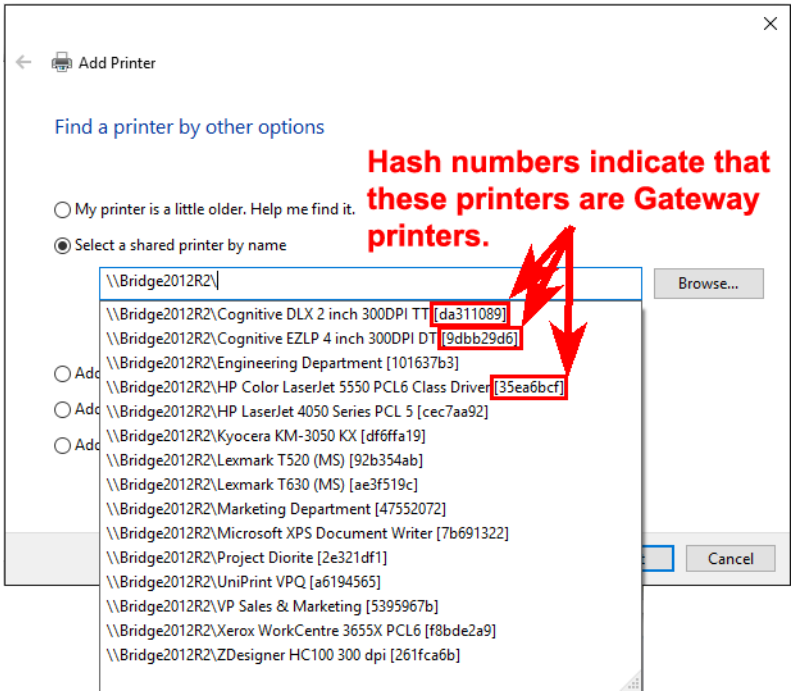


4. Click to select a Gateway printer which are usually indicated with hash numbers. If the printer that you want doesn't appear in the list, click **The printer that I want isn't listed**.

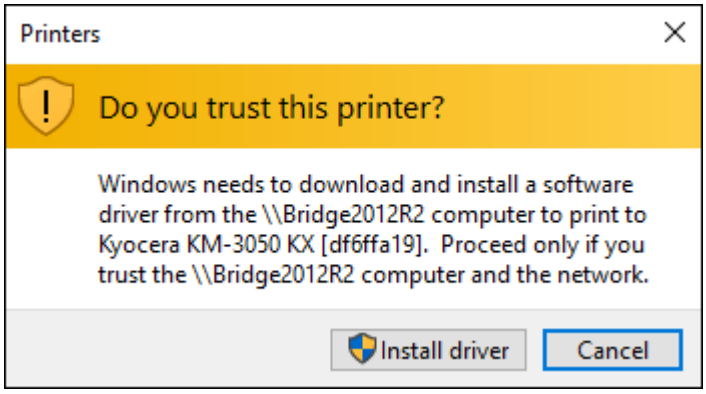


5. Select **A shared printer by name** and then type `\\[BridgeHostName]\`. Click to select a Gateway printer and then click **Next**. Hash numbers are used to ensure that each Gateway

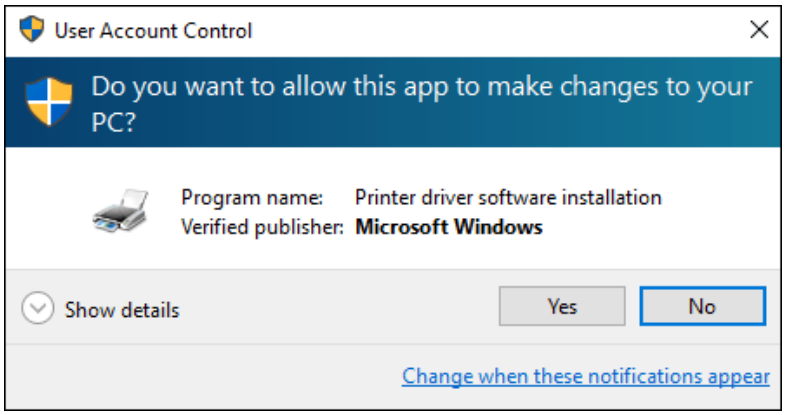
printer is unique and for users they are good indicators that the printer is indeed a Gateway printer.



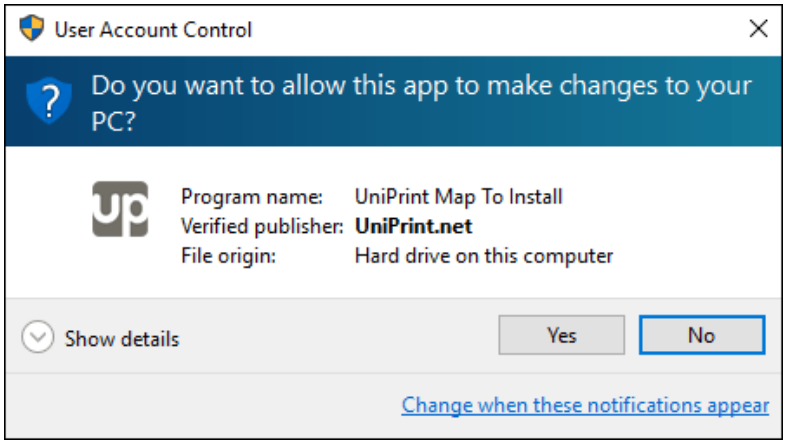
6. Click **Install driver**.



7. Click **Yes**, to clear the UAC message.

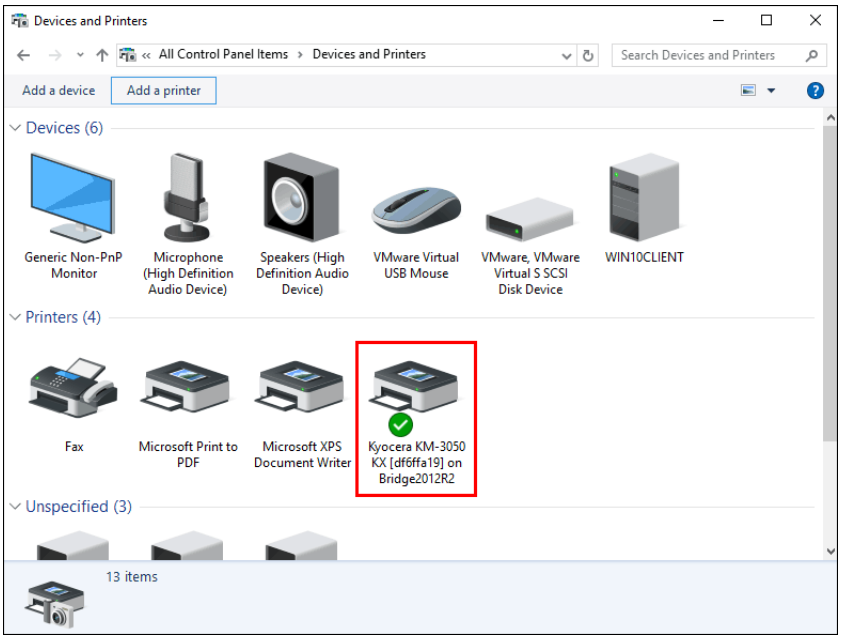


8. Click **Yes** again, to clear the UAC message.



9. Click **Next** and then click **Finish**.

10. The Gateway printer is now available for printing.



NOTE: To remove the One Queue, simply remove the printer and all of the UniPrint components will also be removed from this device.

NOTE: The UniPrint VPQ can also be added in this manner. To release the print at the vPad device, the user needs to enter the user name used to log into their device and the password associated with the print job in order to release to their print job. The domain will be the user's computer name.

Sending Printed Documents as E-mail Attachments

PDF print jobs are sent through the **UniPrint (Email PDF)** printer on the UniPrint Application Server. Before users can send e-mail, the **UniPrint (Email PDF)** printer queue must first be configured and enabled on the UniPrint Application Server through the UniPrint Management Console. For detailed instructions on how to configure and enable the **UniPrint (Email PDF)** queue, see "Enabling & Configuring UniPrint To E-mail Print Jobs as PDF Attachments" on page 129.

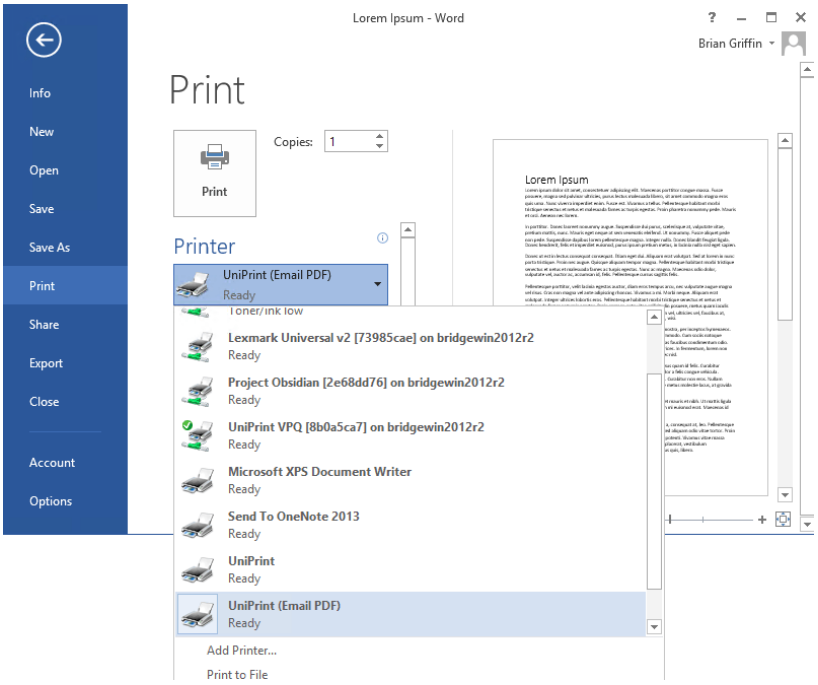
To send the printed document as a PDF attachment, do the following:

1. Log onto the Application Server as you normally would through RDP or ICA to access applications.

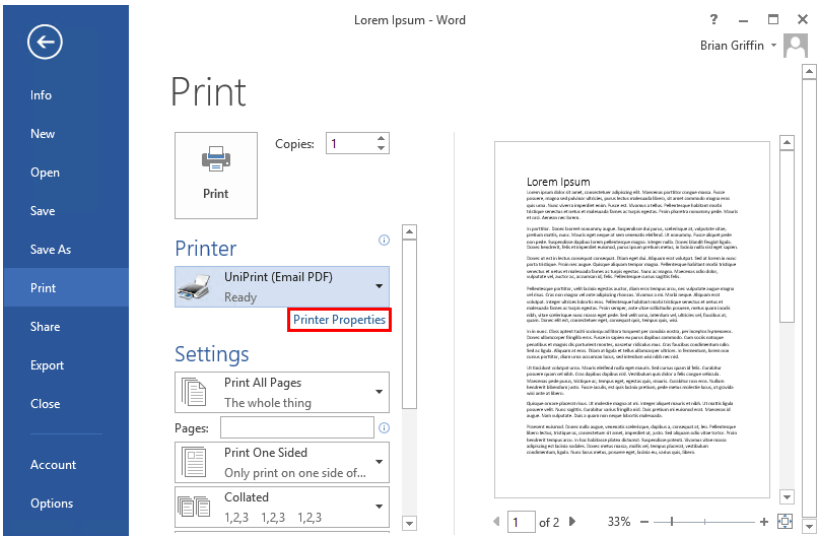
2. Open an application from which to print, for example, Microsoft Word.

3. Print from the application.

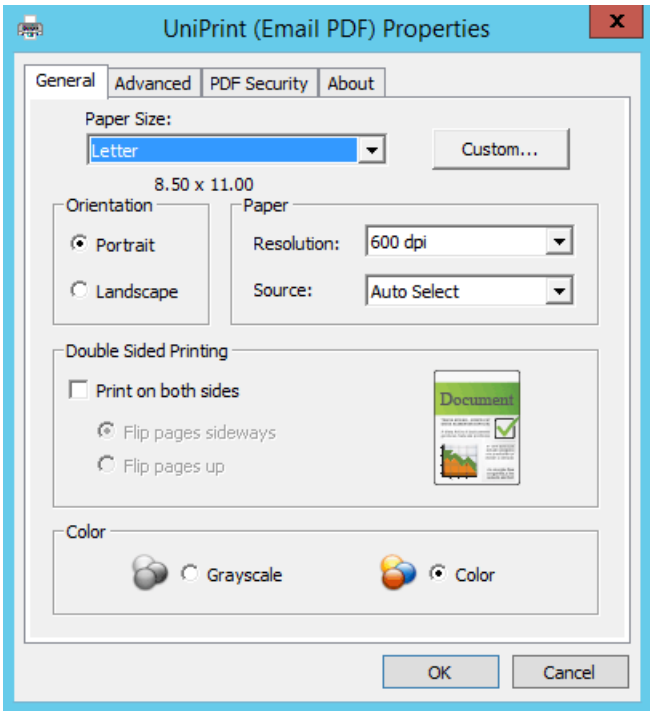
4. Select the **UniPrint (Email PDF)** printer.



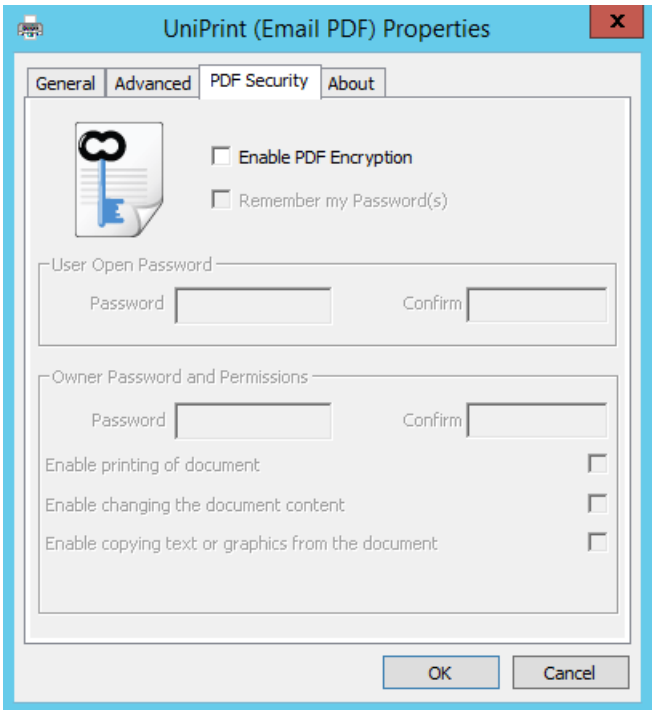
5. To add security to the content of the PDF created, click **Printer Properties**.



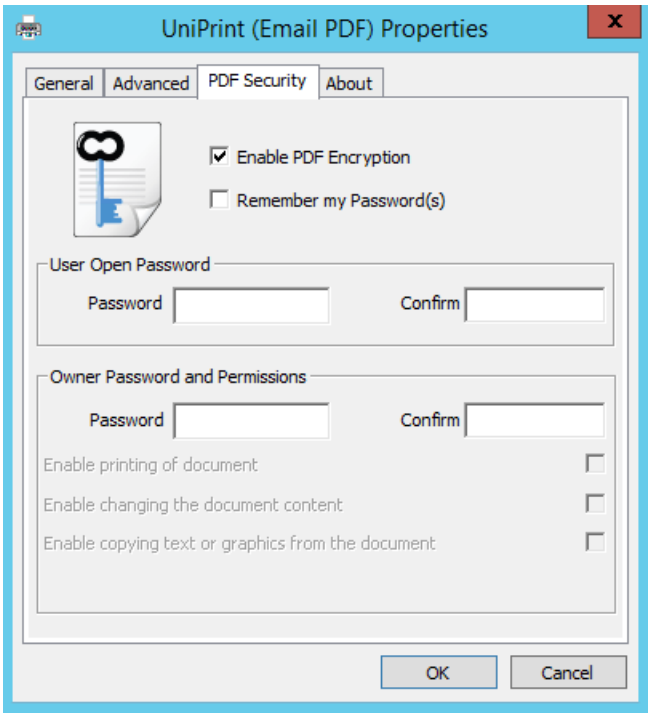
6. To apply password protection and/or to change or restrict certain features to the created PDF file, click the **PDF Security** tab.



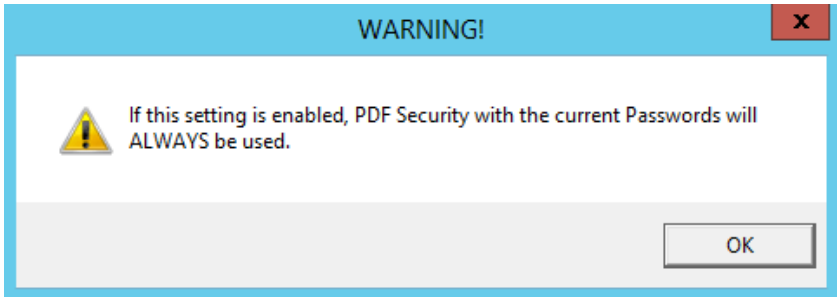
7. Select **Enable PDF Encryption**.



8. If you want your password(s) to remain persistent from session to session, select **Remember my Password(s).**

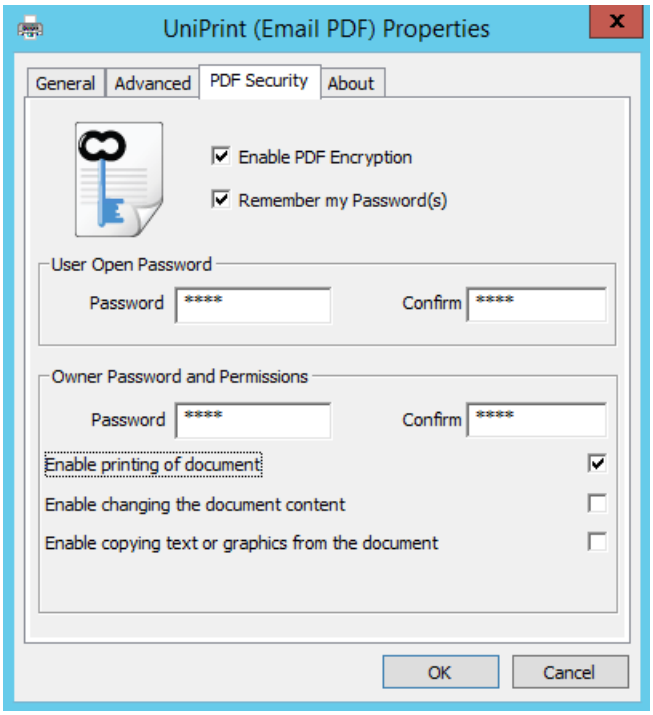


9. A message will appear warning you that PDF security with the current password(s) will be used each and every time you print to the UniPrint (Email PDF) printer. Click **OK.**



BEST PRACTICE: If a password is forgotten, there is no way to recover the password from the PDF file. It is highly recommended that you keep a backup copy of the document that is not password protected.

10. There are two sets of passwords, the **User Open Password** and the **Owner Password and Permissions** password.



User Open Password: With the **User Open Password**, users must type in this password, specified by the sender, to open the PDF document in a PDF reader.

Owner Password and Permissions: The **Owner Password** allows the sender to restrict document features such as printing and editing.

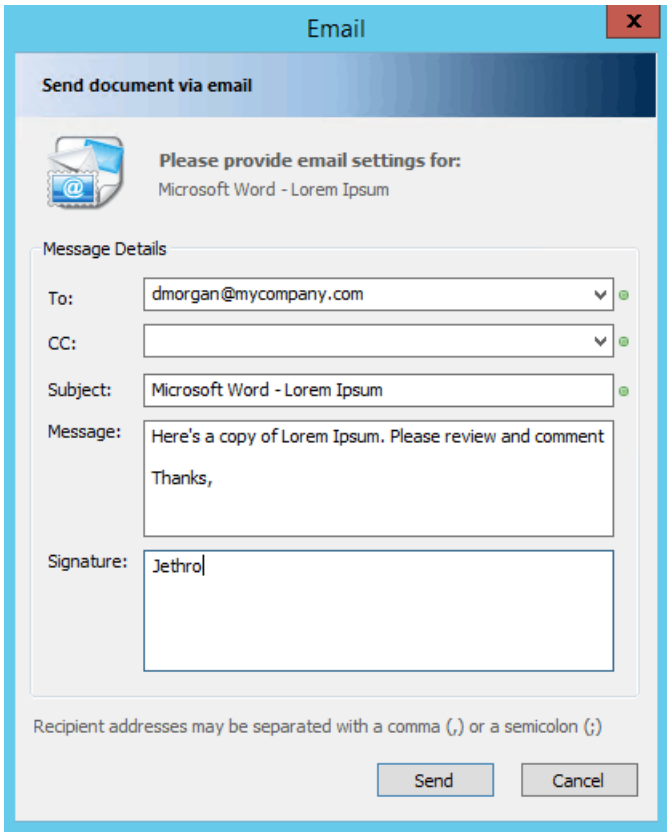
If both types of passwords are set, then the secured PDF can be opened with either password, however, only the Owner Password will allow the user to change which features are restricted in the document.

Enable printing of document	If selected, the user is allowed to print the document.
Enable changing of document content	If selected, the user is allowed to change the contents of the PDF document.
Enable copying of text or graphics from the document	If selected, the user is allowed to copy parts of the text or graphics from the PDF document.

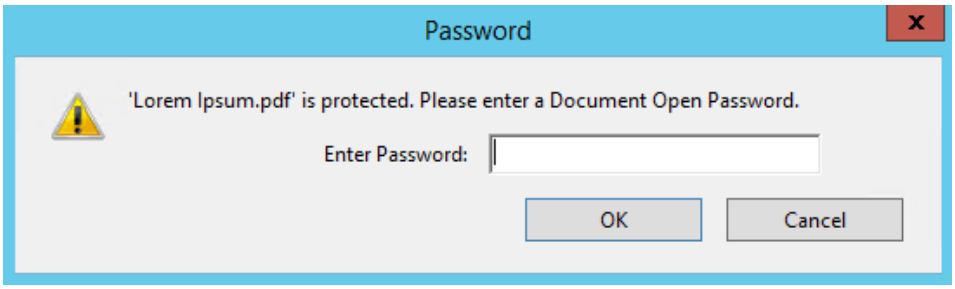
11. After setting passwords and restrictions, click **OK**.

12. Click **Print.**

13. Type in the e-mail address(es) to which to send the printed document, the subject, a short message and your signature and then click **Send**.



14. If PDF Security is enabled, the recipient of the e-mail will be prompted for a password when the attached PDF file is opened.



NOTE: Some third-party products do not support or respect these security settings and document recipients may be able to bypass some or all of these settings.

Saving Printed Documents as PDF Files

There are four ways to save a document as a PDF file in UniPrint Infinity and it depends on whether UniPrint Client is installed on users' workstations or not. The first method is by automatic print job archiving and does not involve any user interaction. For more information on print job archiving, see "Configuring Print Job Archiving" on page 319. The second method is by setting the registry key ShowPreviewPDF to 1 which launches Adobe Reader on the UniPrint Application Server. For more information on configuring this feature, see "Using Adobe Reader to Preview PDF Print Jobs" on page 151. The third method is through the UniPrint Viewer which is outlined in the UniPrint Client User's Guide. The forth method is outlined below and is intended for those who don't have access to the UniPrint Client.

Before users can save their printed documents as PDF files, the **UniPrint (Save PDF)** queue must be enabled on the UniPrint Application Server through the UniPrint Management Console. To enable the **UniPrint (Save PDF)** queue, see "Enabling UniPrint To Save Print Jobs As PDF Files" on page 132.

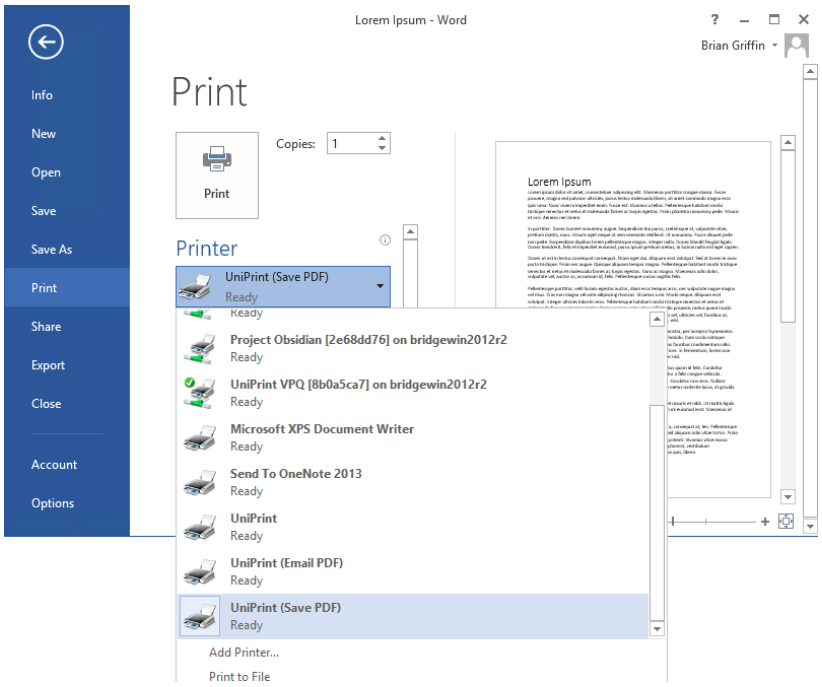
To save printed documents to a network accessible location, do the following:

1. Log onto the Application Server as you normally would through RDP or ICA to access applications.

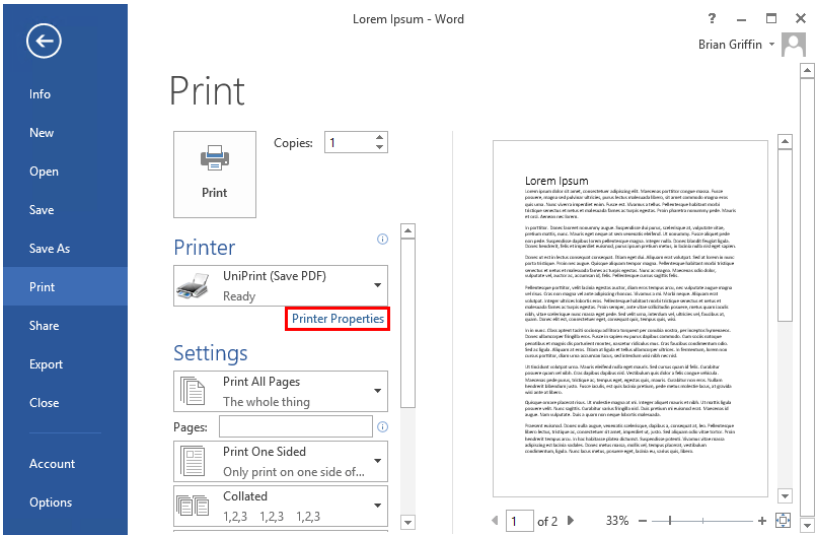
2. Open an application from which to print, for example, Microsoft Word.

3. Print from the application.

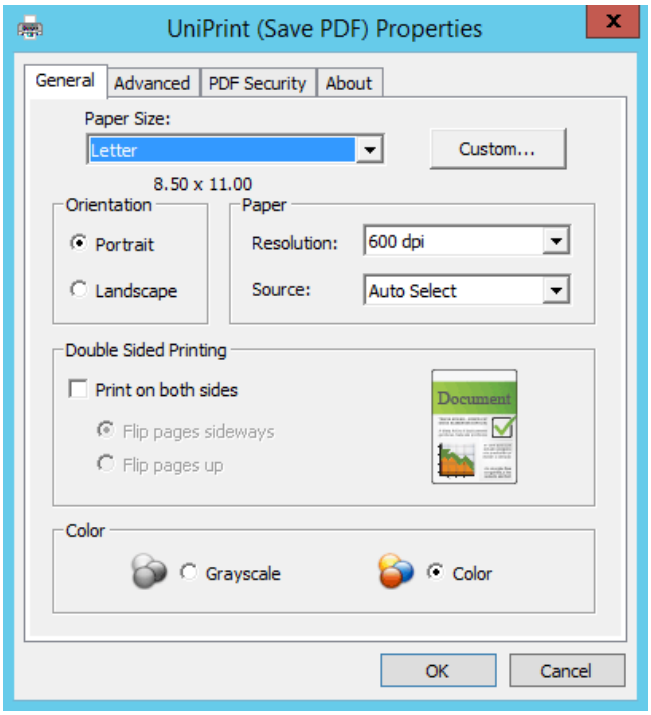
4. Select the **UniPrint (Save PDF)** printer.



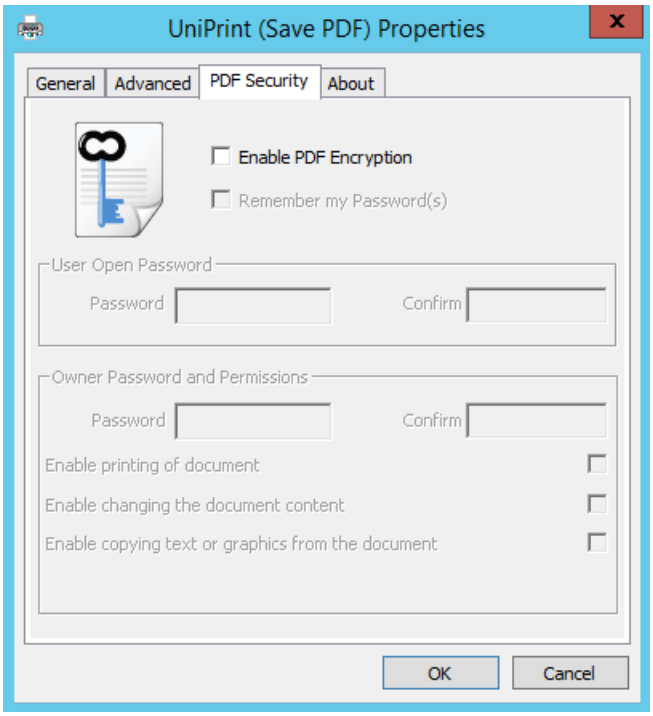
5. Click **Printer Properties**.



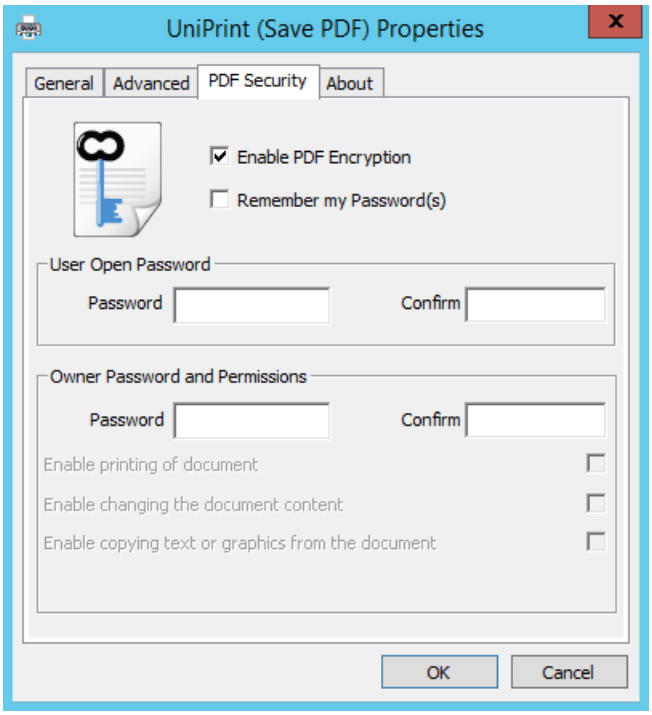
6. To apply password protection and/or to change feature restrictions of the created PDF file, click the **PDF Security** tab.



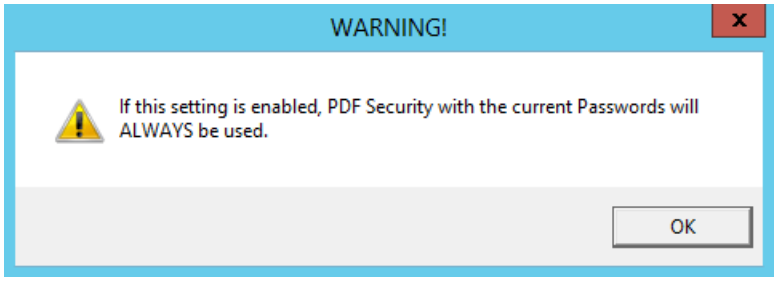
7. Select **Enable PDF Encryption**.



8. If you want your password(s) to remain persistent from session to session, select **Remember my Password(s).**

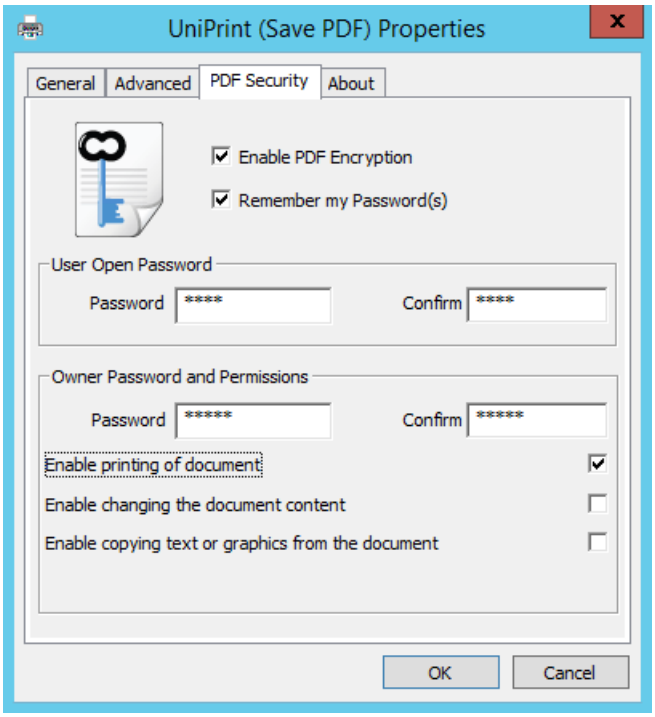


9. A message will appear warning you that PDF security with the current password(s) will be used each and every time you print to the UniPrint (Save PDF) printer. Click **OK.**



BEST PRACTICE: If a password is forgotten, there is no way to recover the password from the PDF file. It is highly recommended that you keep a backup copy of the document that is not password protected.

10. There are two sets of passwords, the **User Open Password** and the **Owner Password**.



User Open Password: With the **User Open Password**, users must type in this password to open the PDF document in a PDF reader.

Owner Password and Permissions: The **Owner Password** allows the sender to restrict document features such as printing and editing.

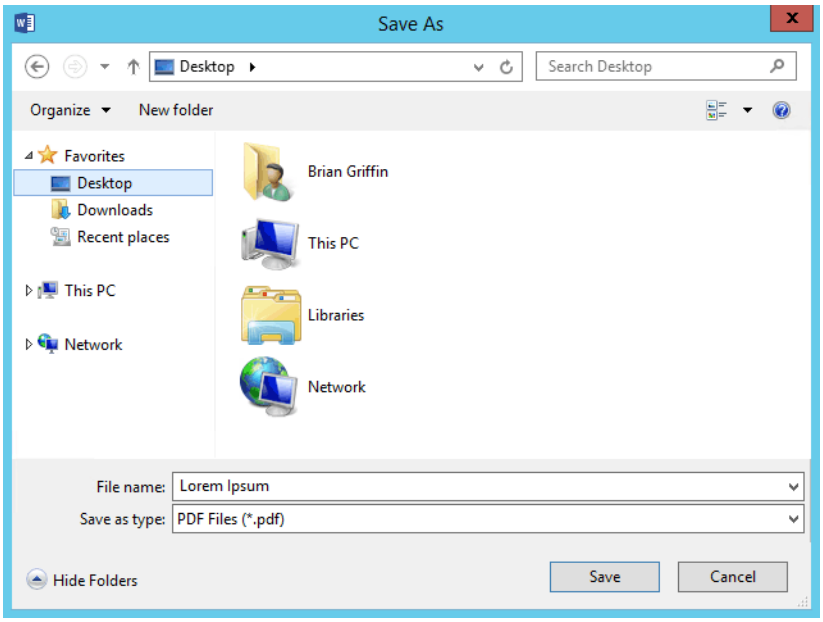
If both types of passwords are set, then the secured PDF file can be opened with either password, however, only the Owner Password will allow the user to change which features are restricted in the document. The User Password and the Owner Password cannot be the same.

Enable printing of document	If selected, the user is allowed to print the document.
Enable changing of document content	If selected, the user is allowed to change the contents of the PDF document.
Enable copying of text or graphics from the document	If selected, the user is allowed to copy parts of the text or graphics from the PDF document.

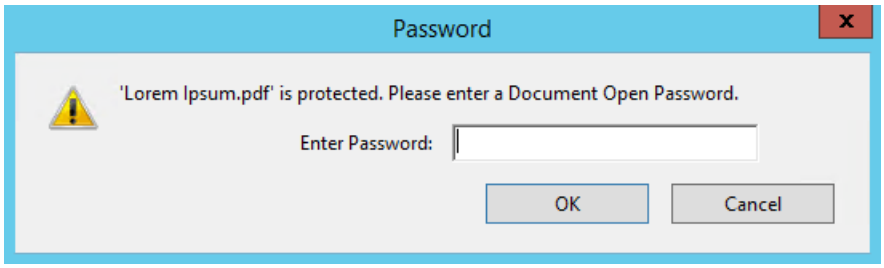
11. After setting the passwords and restrictions, click **OK**.

12. Click **Print.**

13. Browse to a save location, enter a file name and then click **Save**.



14. If PDF Security is enabled, the user will be prompted for a password when the PDF file is opened.



NOTE: Some third-party products do not support or respect these security settings and document recipients may be able to bypass these settings.

Using Printer Profiles to Print With Advanced Printer Properties

Printer profiles can be used to access and group together advanced printer properties like double-sided printing, stapling and hole punching since it uses the printer's native printer driver. They are also convenient since a user can select a combination of printer properties with just one click.

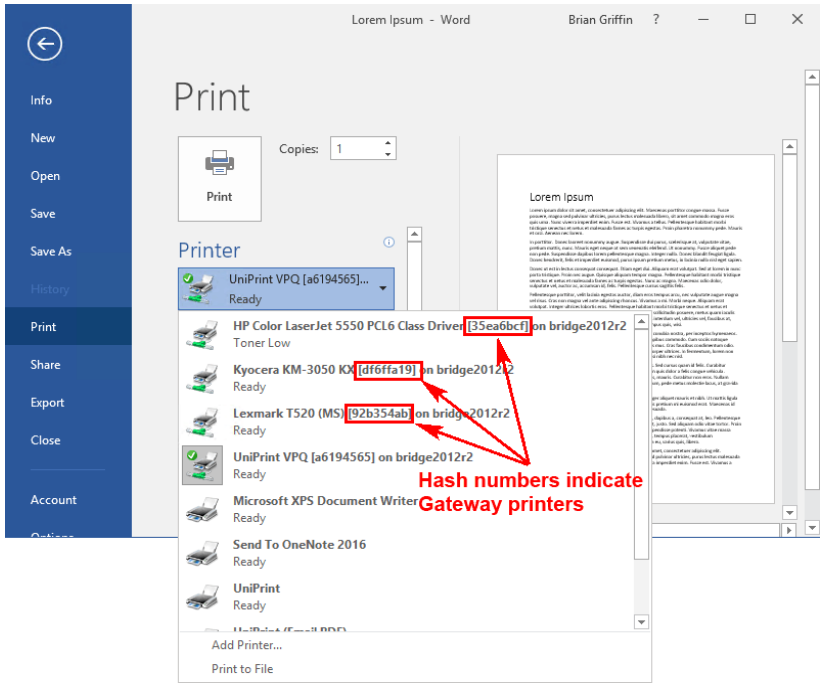
To print with a printer profile, do the following:

1. Log onto the Application Server as you normally would through RDP or ICA to access applications.

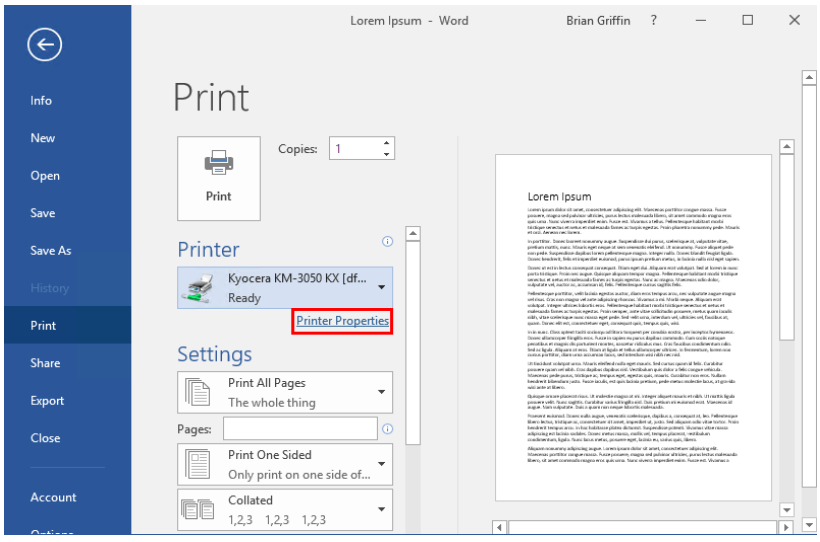
2. Open an application from which to print, for example, Microsoft Word.

3. Print from the application.

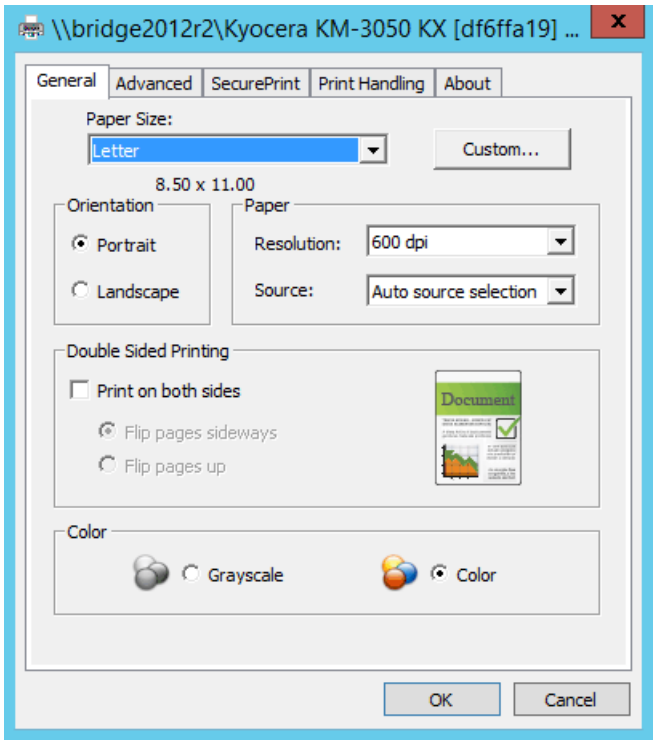
4. Click to select a Gateway printer.



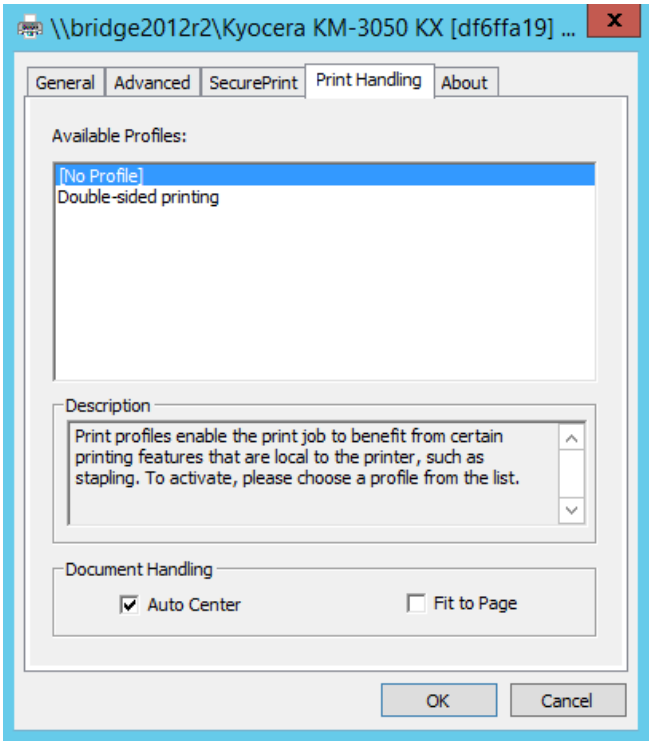
5. Click **Printer Properties**.



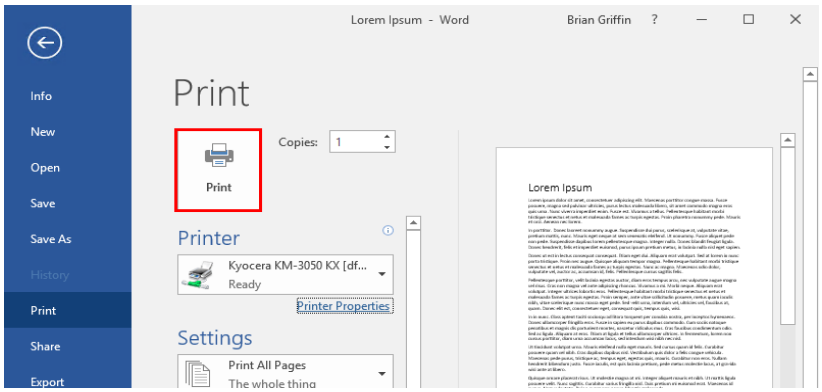
6. Click the **Print Handling** tab.



7. Click to select a profile and then click **OK**.



8. Click **Print** and the document will be printed according to the selected profile.



Printing PDFs from Adobe Acrobat or Reader

Documents that are already in PDF format need to be printed through the Adobe Plug-in. The Adobe Plug-in notifies UniPrint not to re-render the PDF which will result in substituted or missing fonts.

In Adobe Acrobat and Reader X and later, the interface has changed compared to earlier versions. Therefore, the Adobe Plug-in appears in different places depending on the version of Acrobat or Reader that is installed. Provided are three sets of instructions, one for Adobe Acrobat/ Reader 9 and earlier, one for Adobe Acrobat/Reader X and XI and another for Adobe Acrobat Reader DC.

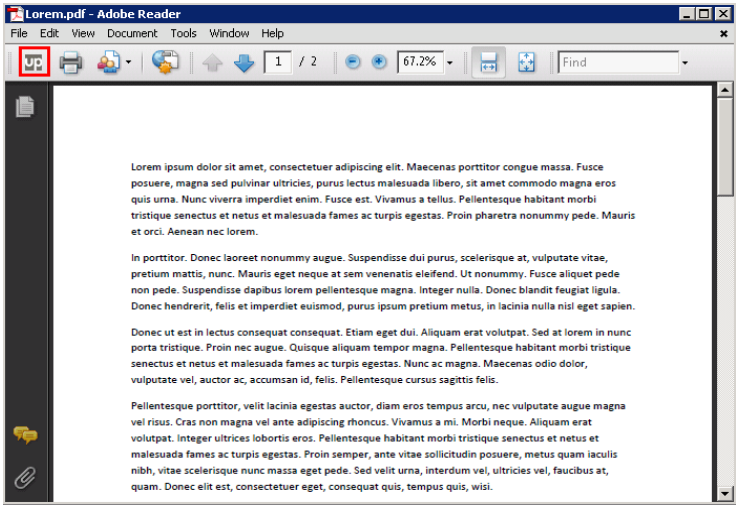
Printing PDFs from Adobe Acrobat or Reader 9

To print a file that is already in PDF format in Adobe Acrobat/Reader 9 or earlier, do the following:

1. Log onto the Application Server as you normally would through RDP or ICA to access applications.

2. Open the PDF document that you want to print.

3. Click the UniPrint icon or in the **File** menu, click **Print to UniPrint**.



4. Select the desired printer and printer properties and then click **OK**.

Printing PDFs from Acrobat or Reader X or XI

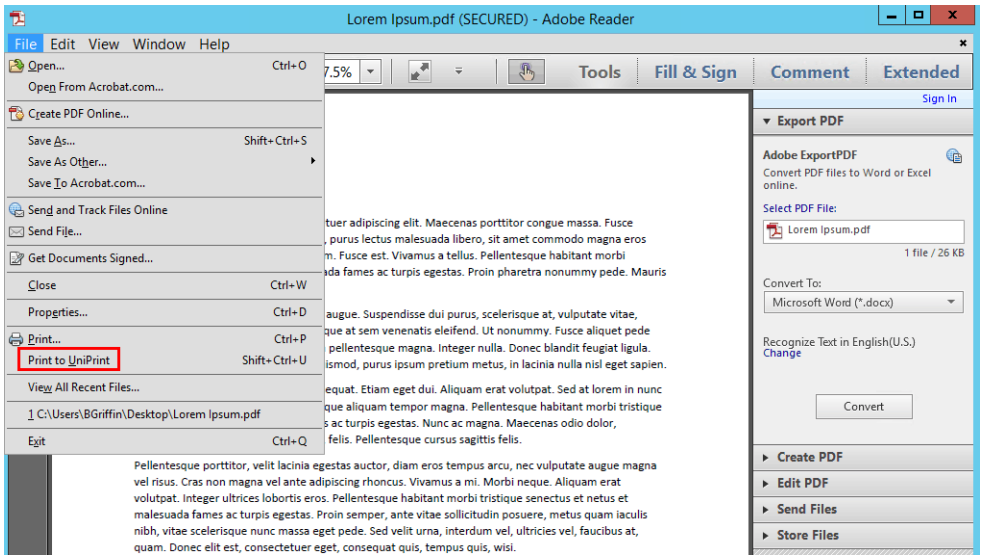
> Prior to printing with the Adobe Plug-in, in Reader XI or later, either disable the **Enable Protected Mode at startup** option or whitelist the Adobe Plug-in. For detailed instructions, see "Enabling the UniPrint Adobe Plug-in to run with Adobe Reader XI & Later" on page 147.

In Adobe Acrobat/Reader X or XI, do the following:

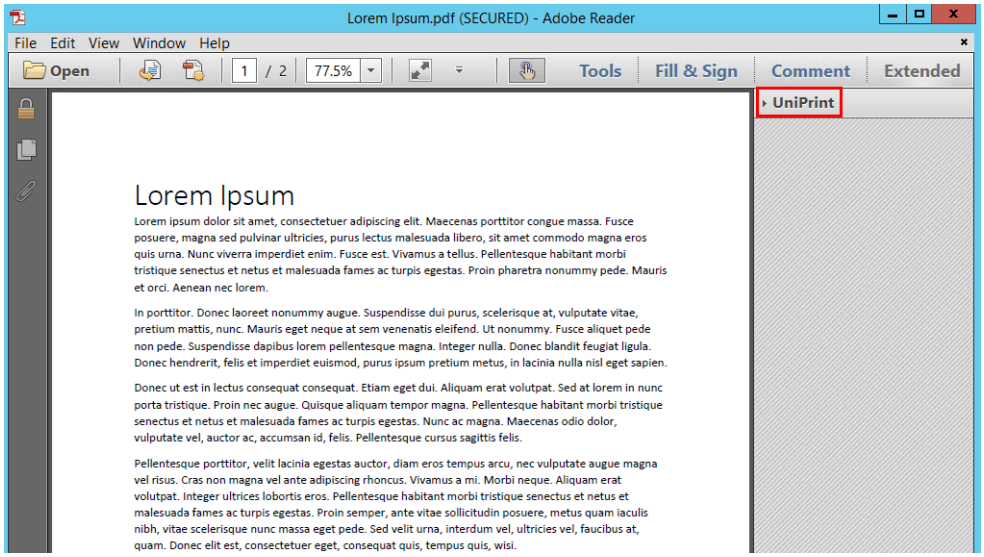
1. Log onto the Application Server as you normally would through RDP or ICA to access applications.

2. Open the PDF document that you want to print.

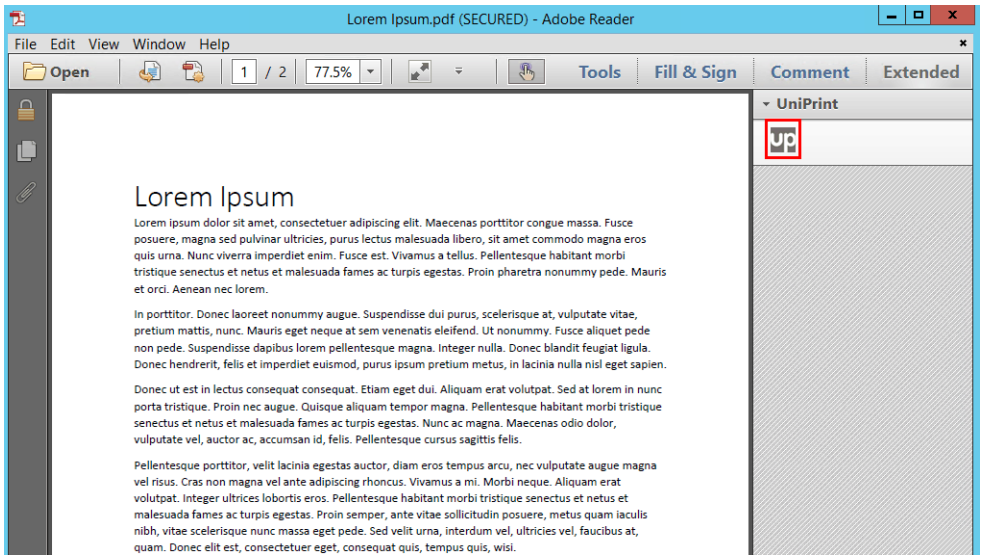
3. From the **File** menu, click **Print to UniPrint**.



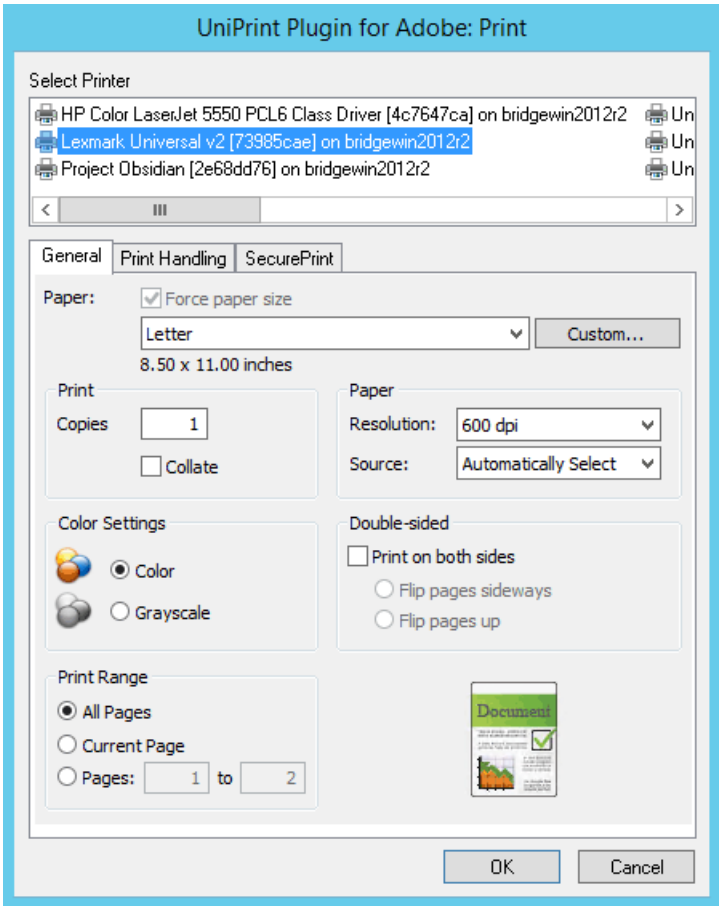
a) Or click **Extended** and then click **UniPrint**.



b) Click the UniPrint icon.



4. Click to select the desired printer and printer properties and then click **OK**.



Printing PDFs from Acrobat Reader DC or later

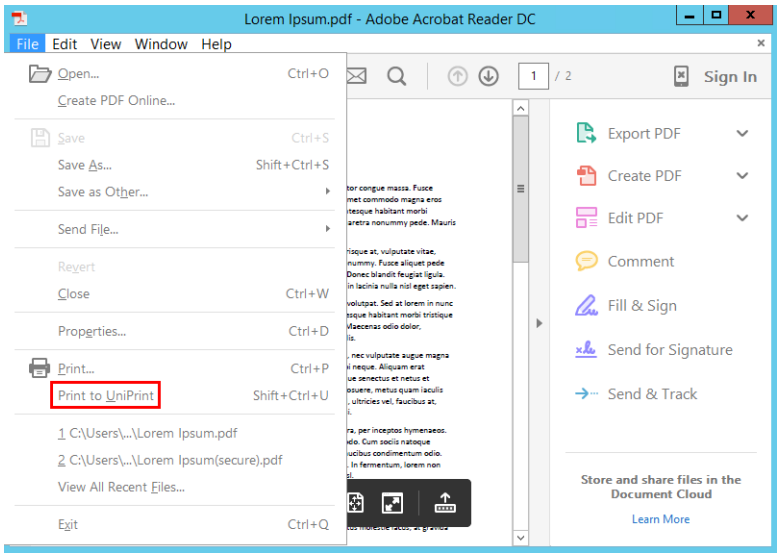
NOTE: Prior to printing with the Adobe Plug-in, in Acrobat Reader DC, either disable the **Enable Protected Mode at startup** option or whitelist the Adobe Plug-in. For detailed instructions, see "Enabling the UniPrint Adobe Plug-in to run with Adobe Reader XI & Later" on page 147.

In Adobe Acrobat Reader DC, do the following:

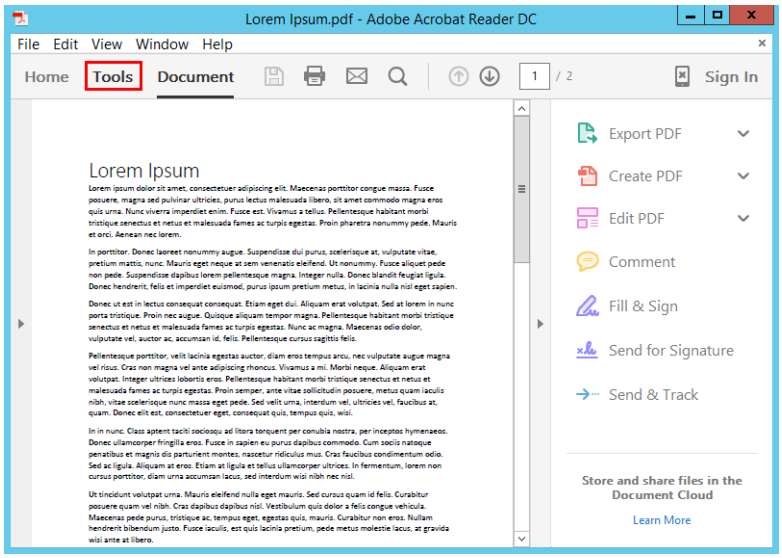
1. Log onto the Application Server as you normally would through RDP or ICA to access applications.

2. Open the PDF document that you want to print.

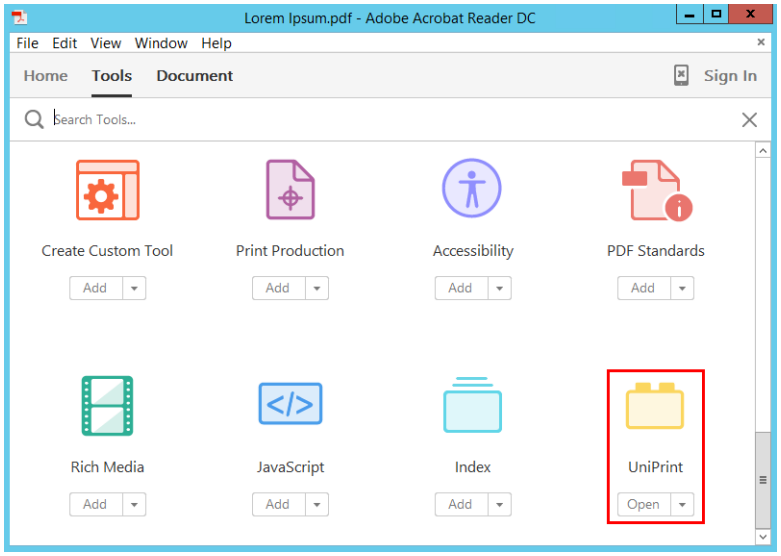
3. From the **File** menu, click **Print to UniPrint**.



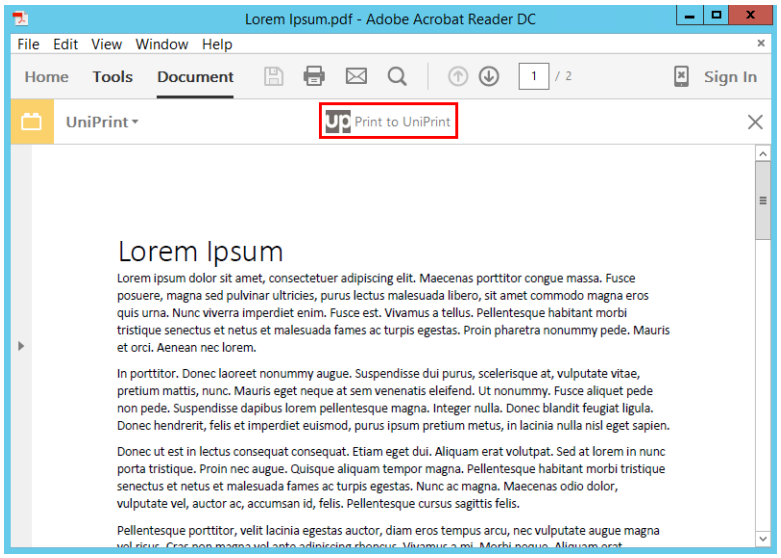
a) Or click **Tools**.



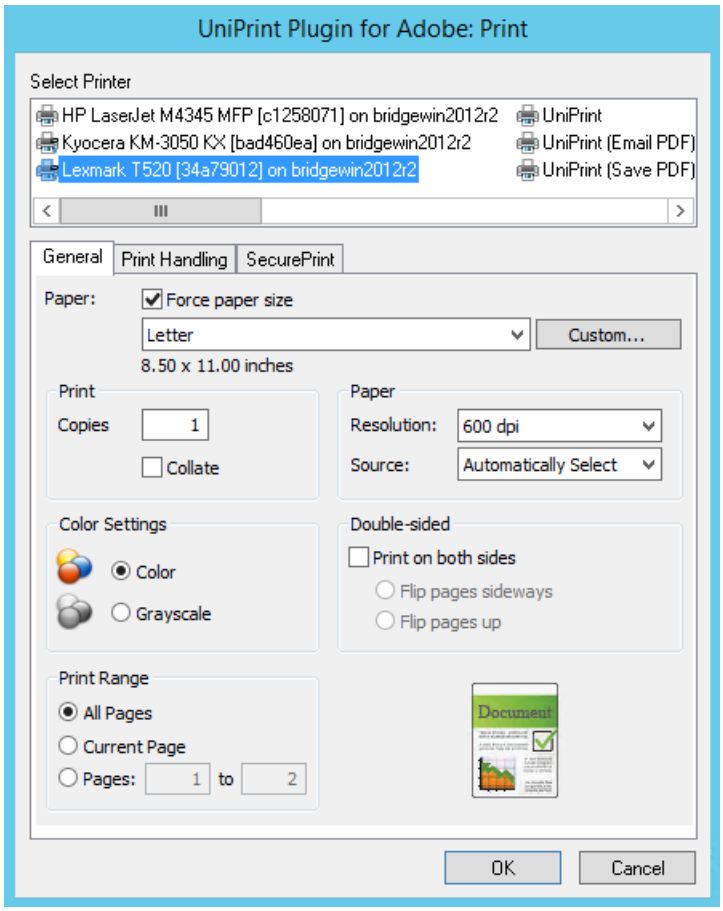
b) And then click **UniPrint**.



c) Click **Print to UniPrint**.

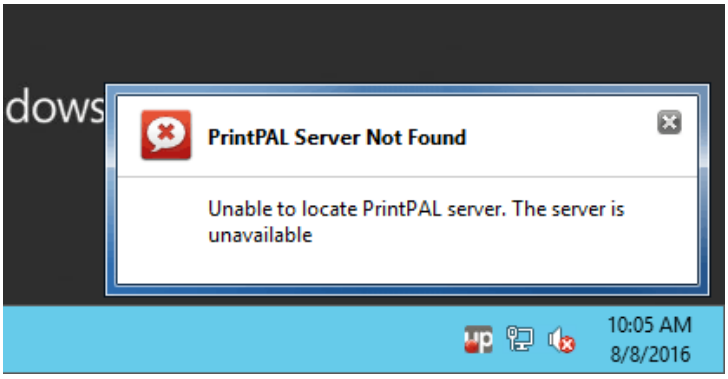


4. Click to select the desired printer and printer properties and then click **OK**.



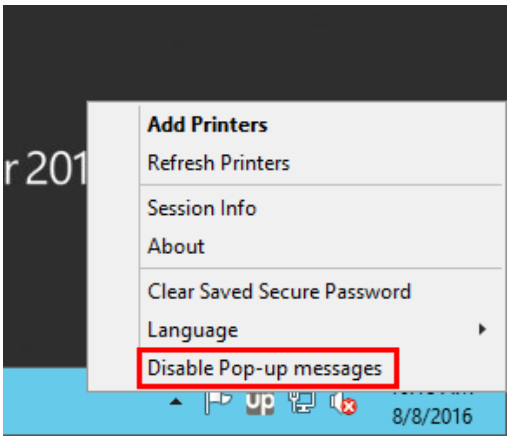
Disabling Pop-up Messages When Not Logged In

This feature was originally designed for mobile users who don't always log into their Application Server while travelling. When a user session is unable to connect to the Bridge, a pop-up message appears.



To prevent any UniPrint Infinity pop-up messages, do the following,

1. In the notification area, right-click .
2. Select **Disable Pop-up messages** and when the user next logs in, UniPrint Infinity messages will no longer pop-up.



CHAPTER 12

UniPrint Infinity

Contact and Support

UniPrint Support

Contact us if you require assistance with any of the UniPrint products.

North America

Hours of Operation
08:00 to 18:00 Central Time (UTC -6)
Monday to Friday

Toll Free Phone Number (North America Only)
1-866-488-3188 option 3

Phone Number
+1 (416) 848-0329 (Worldwide)

Europe, Middle East and Africa

Hours of Operation
08:00 to 18:00 Coordinated Universal Time (Greenwich Mean Time)
Monday to Friday

Phone Number
+44 1344 206144

E-mail

support@uniprint.net

Office Location

Address

UniPrint.net Corp.
1420-3280 Bloor St. W., Centre Tower
Toronto, ON M8X 2X3
Canada

Phone Number
(416) 503-9800

Toll Free Phone Number (North America Only)
1-866-488-3188

ADDENDUM **A**

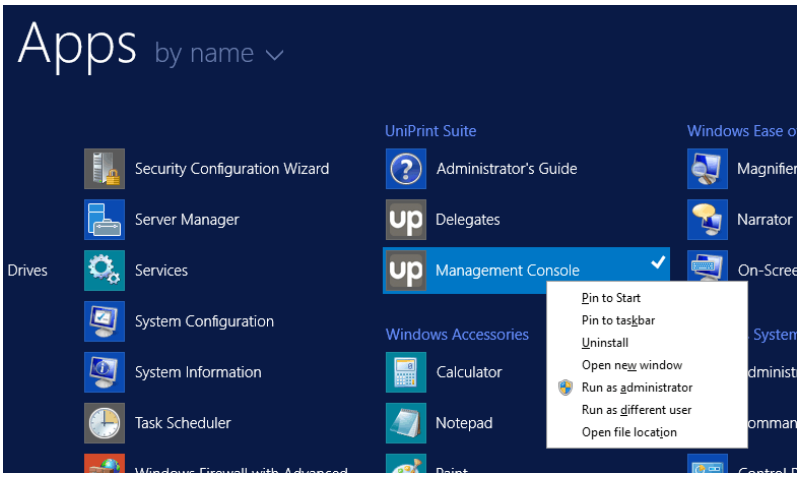
UniPrint Infinity

UniPrint Management Console Interface

The UniPrint Management Console is a container for configuration tools and utilities and is installed on each UniPrint component. This addendum describes all the available settings and options of the UniPrint Management Console. For the most part, the UniPrint Management Console is the same on each UniPrint component server, with three exceptions. Printer Profiles are only installed on the UniPrint Print Server. PrintPAL Server is installed on the UniPrint Bridge but is also accessible for configuration on the UniPrint Application Server. Sessions only applies to and is accessible from the UniPrint Application Server.

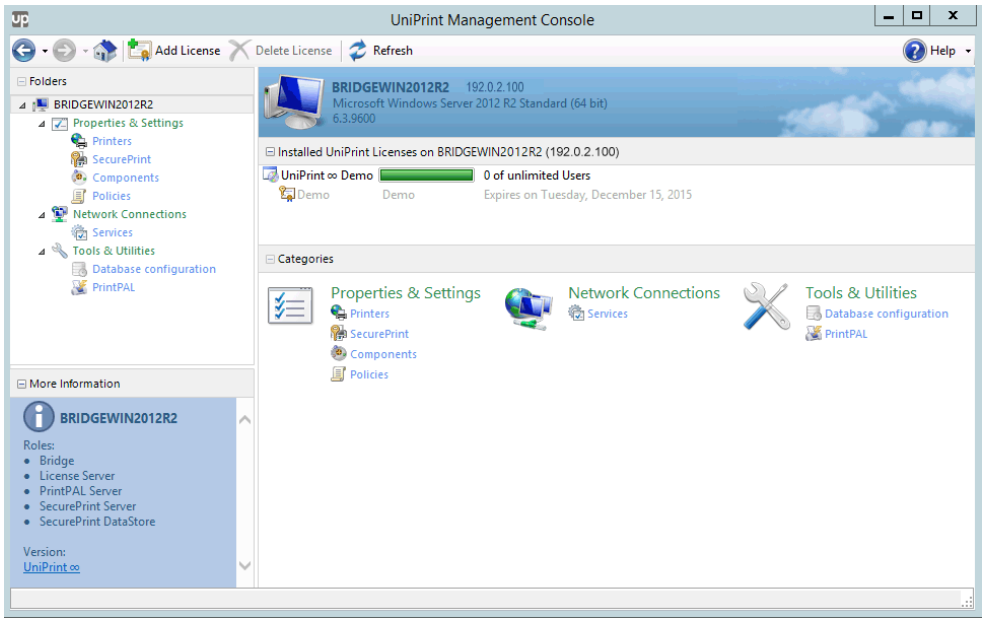
To start the UniPrint Management Console, on any UniPrint component server, do one of the following:

- Click **Start**, click and then click **Management Console**. To pin it to the **Start** menu or taskbar, right-click **Management Console** and then select **Pin to Start** or **Pin to taskbar**.



- Alternatively, the console (UPConsole.exe) can be launched from the application folder, for example, C:\Program Files\UniPrint Suite\Console.

Console Home



From the **Console Home** screen, the top banner displays information such as server name, IP address and operating system. You also have access to the license server and can add licenses or view real time license usage. Additionally, you can take a detailed snapshot of license usage.

Under **Properties & Settings**, you have access to the following settings:

Configuration Screen	Description
Printers	Use this screen to manage printers installed on both the UniPrint Bridge and on the UniPrint Print Server(s).
SecurePrint	Use this screen to manage UniPrint vPad devices and their corresponding print queues.
Components	Use this screen to configure UniPrint component properties and to access debugging logs. The components displayed differ depending on which UniPrint component server is being accessed.
Policies	Use this screen to manage how Group Policy Objects affect UniPrint settings.

Under **Network Connections**, you have access to the following settings:

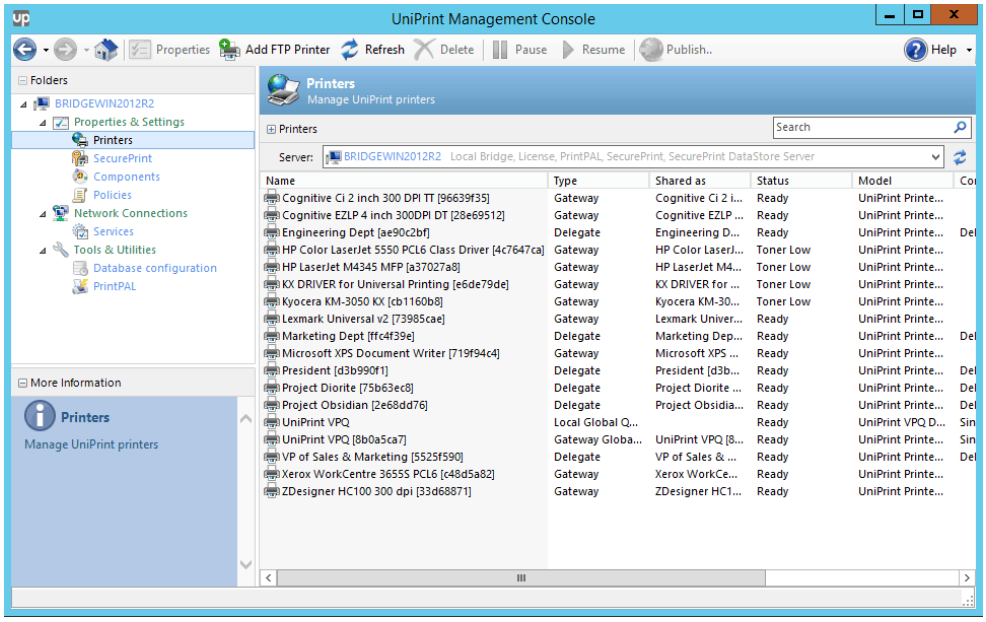
Configuration Screen	Description
Sessions	This screen is only accessible from the UniPrint Application Server. From this screen you can configure how UniPrint interacts with user sessions.
Services	From this screen you can configure local UniPrint services. The services displayed differ depending on which UniPrint component server is being accessed.

Under **Tools & Utilities**, you have access to the following:

Configuration Screen	Description
Database configuration	This utility is used to connect to a central database other than Firebird which is installed with UniPrint. For most setups, Firebird is recommended. However, for high availability setups, administrators have the option to connect an external, centralized database.
PrintPAL	This utility is only accessible from the UniPrint Bridge and UniPrint Application Server components and is used to manage session printer mappings.
Printer Profiles	This utility resides on the UniPrint Print Server and is used to access and group advanced printer properties such as stapling and hole punching.

Properties & Settings

Printers



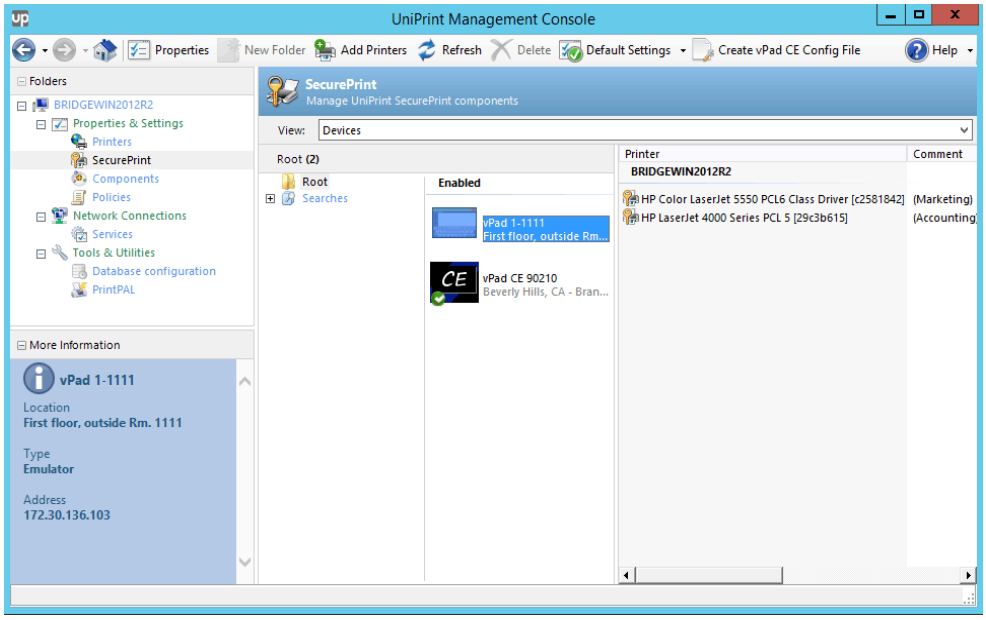
Printers is accessible from all UniPrint component servers, however different settings can be configured on different UniPrint components. To select a different UniPrint component server, beside **Server**, click the drop-down arrow and select a different server.

On the UniPrint Bridge, administrators have the ability to change the default Gateway printer properties, delete a Gateway printer, pause an available Gateway printer and create new FTP printer instances. For label printers, Page Description Languange (PDL) support can also be enabled on the UniPrint Bridge.

From the UniPrint Print Server, administrators can add new Gateway printers, publish them to the UniPrint Bridge, specify and change naming conventions for published Gateway printers, and manage Printer Profiles.

On the UniPrint Application Server, the UniPrint printer, UniPrint (Email PDF) and UniPrint (Save PDF) printer queues can also be configured and enabled. To edit the properties of a UniPrint printer queue, click to select it and then click **Properties**.

SecurePrint



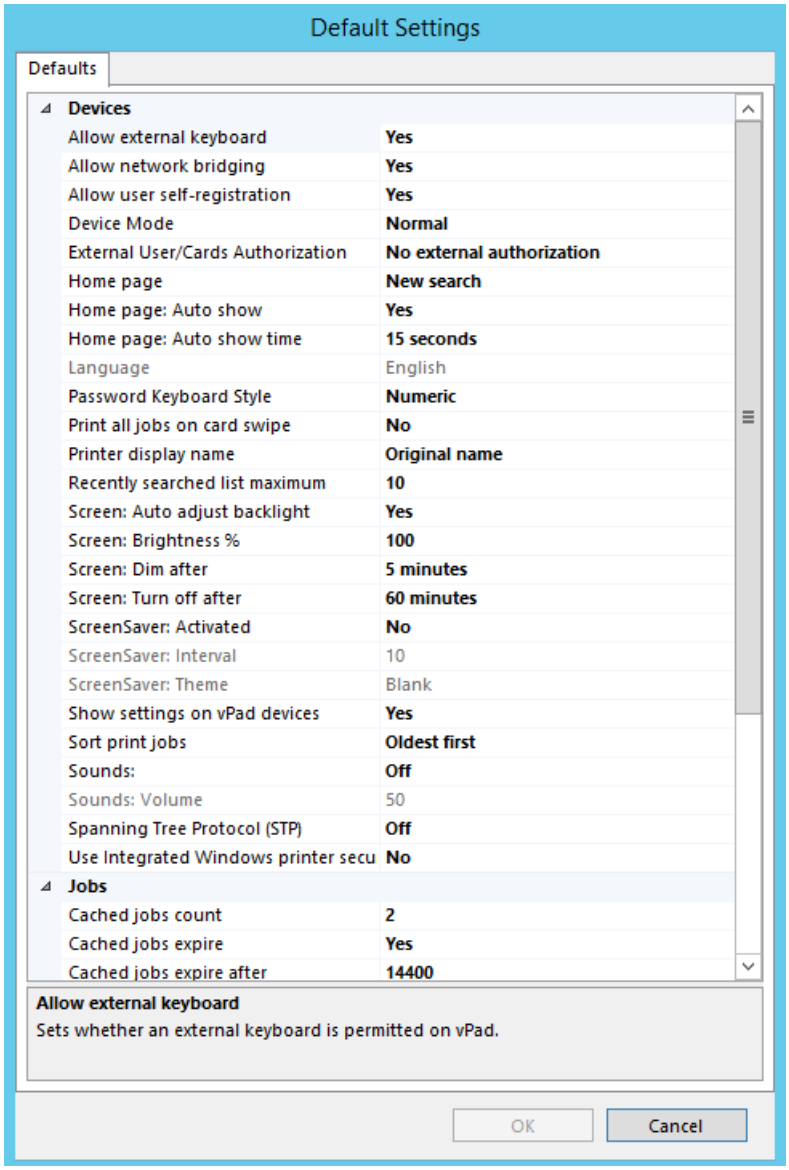
SecurePrint is accessible from all UniPrint component servers, but initial configuration should be done on the UniPrint Bridge. SecurePrint will auto-discover any vPad device that is attached to your network.

From this screen, you can enable vPad devices, change their properties and assign Gateway printers to them. If this UniPrint component server is also your SecurePrint Data Store, you can also set vPad properties globally for all devices, by clicking **Default Settings.**

Depending on your network, the vPad CE may not be discovered by the UniPrint Management Console. Click **Create vPad CE Config File** to create a config file on a USB flash drive which can the be inserted in the vPad CE device. For detailed instructions, see "Configuring the vPad CE to Connect to the UniPrint Print Server" on page 208.

A list of users and their corresponding smart card ID numbers can also be imported and registered through this screen.

Default Settings



Setting	Description
Allow external keyboard	If set to **Yes**, then a USB keyboard can be attached to the vPad device. This setting does not apply to the SecurePrint Emulator. Default is **Yes**.
Allow network bridging	If set to **Yes**, then network bridging is permitted on this vPad device. This setting does not apply to the SecurePrint Emulator. Default is **Yes**.

Setting	Description
Allow user self-registration	If set to **Yes**, after the user submits a print job with a password, the user can then register their contact-less proximity smart card or a contact smart card with a magnetic strip through the vPad device in order to associate their user name to their smart card.
Delegated print job notification	If set to **Yes**, a notification bar will appear on the specified vPad device notifying users that a delegated print job is available for printing. The default is **Yes**.
Device Mode	Sets how users can retrieve print jobs from the vPad device. The options are Normal and Locked down. If set to **Locked down**, the device will be unresponsive to touch until a valid smart card or magnetic strip is used.
External User/Cards Authorization	Sets the external authorization method to be used for authentication. Third-party single sign-on and password management systems, such as Imprivata OneSign can be integrated into SecurePrint. The available options are: • **No external authorization** - Use a combination of domain username/ password or RFID/HID to access the vPad and then a print job specific SecurePrint password to release the print job. • **Imprivata with external reader** - Use an Imprivata proximity card on an external card reader to authenticate the user and release print jobs with a SecurePrint password. • **Imprivata with internal reader** - Use an Imprivata proximity card with the vPad internal card reader to authenticate the user and release print jobs with a SecurePrint password. Default setting is **No external authorization**.

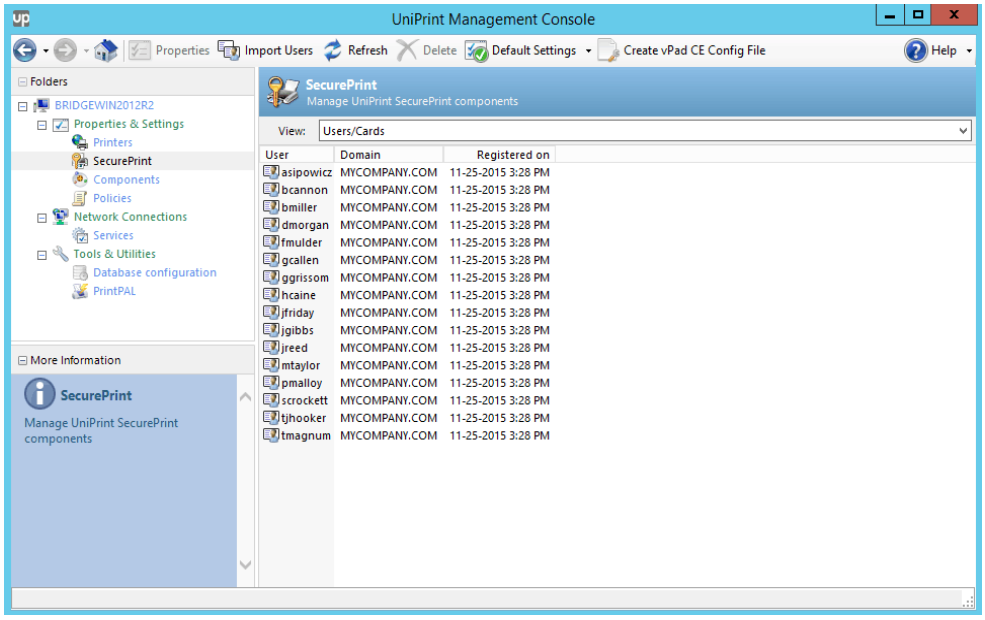
Setting	Description
Home page	If set to **NewSearch**, users will be required to enter their user name in order to display their print jobs. If set to **RecentUserList**, users can scroll and select from a list of users who recently sent a print job, but have not retrieved it. **NewSearch** is the default Home page.
Home page: Auto show	If set to **Yes**, the default Home page will be displayed after a period of inactivity.
Home page: Auto show time	Sets the amount of time the vPad needs to be inactive before the screen changes to the default Home page. Available options are 15 seconds, 30 seconds, 1 minute, 2 minutes, and 5 minutes.
Language	English, French, German, Italian, Polish and simplified Chinese interfaces are now available.
Password Keyboard Style	Sets the default keyboard style that appears when the user is prompted to enter their password. Available options are **Numeric** and **Alphabetic**. The default style is **Numeric**.
Print all jobs on card swipe	If set to **Yes**, all active print jobs are sent to print to an assigned default printer when a card is swiped. If a default printer is not set, the user will be presented with a list of available printers.
Printer display name	Sets how printer names are displayed on the vPad. Available options are Original name and UniPrint Gateway name.
Recently searched list maximum	Sets the maximum number of user names displayed in the recently searched list.
Screen: Auto adjust backlight	If set to **Yes**, the screen will dim and then turn off automatically after a set amount of inactive time.
Screen: Brightness %	Sets the percentage of brightness. The default is 100%.

Setting	Description
Screen: Dim after	The vPad screen will dim, if it is inactive for the amount of time set here. Available options are 30 seconds, 1 minute, 2 minutes, 5 minutes, 10 minutes and 20 minutes.
Screen: Turn off after	The vPad screen will turn off, if it is inactive for the amount of time set here. Available options are 5, 10, 15, 20, 30, and 60 minutes.
ScreenSaver: Activated	If set to **Yes**, a screensaver will run on the vPad after a period of inactivity.
ScreenSaver: Interval	A screensaver will activate, if the vPad is inactive for the amount of time set here in seconds.
ScreenSaver: Theme	The theme can either be set **Blank** in which the screen turns off or to **Fading** where the UniPrint logo floats in different directions on the screen.
Server Connection: Static address:port	The static IP address and port number for the print server to which the vPad is connected can be added. ***Note**: The port number must be included.*
Show settings on vPad devices	If set to **Yes**, the Settings icon and screen will be available on the vPad device and any user can change its settings.
Sort print jobs	Print jobs can either be displayed with the oldest first or the newest first.
Sounds	Tap sounds can be enabled or disabled.
Sounds: Volume	The volume can be set between 0 and 100%. The default is 50%.

Setting	Description
Spanning Tree Protocol (STP)	This setting is only applicable to the vPad device itself and does not apply to the Emulator. The vPad device has two network ports. One port should be connected to your network and the other port is intended to be connected to a network printer. However, if it is deemed necessary to connect both ports to the network, a bridge loop may be created resulting in broadcast radiation. To prevent this from occurring, set this setting to **On**. Default is **Off**.
Use Integrated Windows printer security	If set to **Yes**, SecurePrint will check Group Policies and display only the printers to which the user has access.
Cached jobs count	Sets the number of print jobs per user to keep cached in history. Default is 2.
Cached jobs expire	Sets whether cached jobs expire. If set to **Yes**, cached jobs will expire after the time set in **Cached jobs expire after**. If set to **No**, cached jobs never expire and will remain in the cached history until they are manually removed. Default is **Yes**.
Cached jobs expire after	Sets how long (in minutes) cached jobs are kept. Default is 14400 minutes (10 days).
Cached jobs expiry check	Sets how frequently (in minutes) the system checks for expired cached jobs. Default is 60 minutes.
Unclaimed jobs expire	Sets whether unclaimed jobs expire. If set to **Yes**, unclaimed jobs will be deleted after the time set in **Unclaimed jobs expire after**. If set to **No**, unclaimed jobs never expire and will remain in queue until they are manually deleted. Default is **No**.
Unclaimed jobs expire after	Sets how long (in minutes) unclaimed jobs are kept. Default is 1440 minutes (24 hours).
Unclaimed jobs expiry check	Sets how frequently (in minutes) the system checks for unclaimed jobs. Default is 60 minutes.

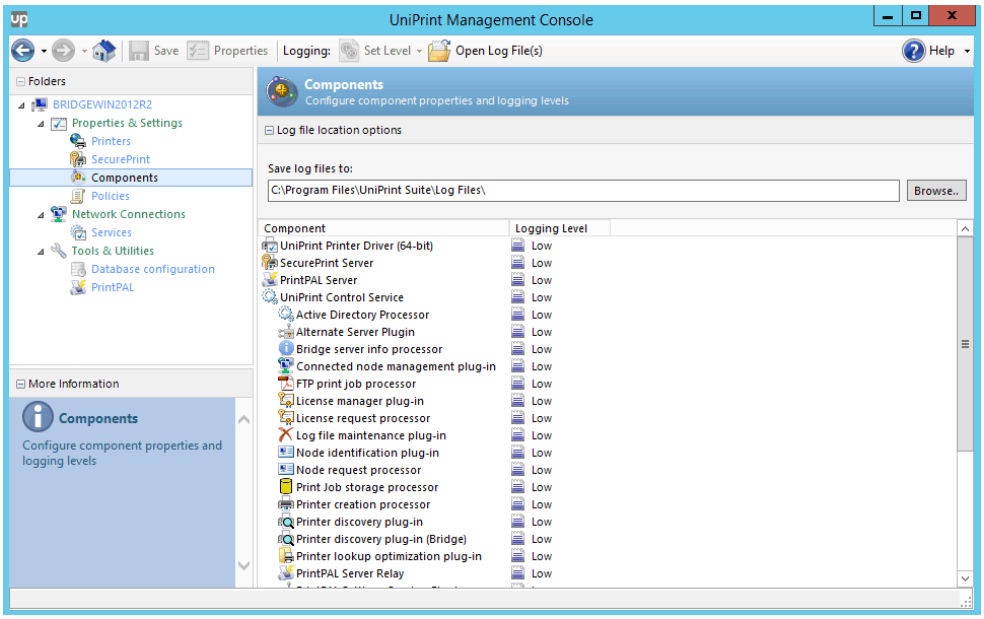
Setting	Description
Require vPad password	If set to **Yes**, the user will be required to set and enter a password in order to release their print job.
Require VPQ password	If set to **Yes**, whenever the user prints to the UniPrint VPQ (virtual print queue), the user will be required to set and enter a password in order to release their print job.
Allow password bypass at device	This is for valid smart card, RFID or HID users. If set to **Yes**, only the smart card, RFID or HID is required for authentication and release of print jobs. If set to **No**, using the smart card, RFID or HID will only display the user's list of print jobs. However, the user will still be required to enter a password in order to release a print job.
Maximum print job password retry attempts	Sets the number of SecurePrint password attempts allowed on the vPad in order to release the print job. If the user exceeds the number of attempts set here, the print job is deleted and the user will have to print their document again and set another SecurePrint password. To set the number of attempts to unlimited, set this setting to 0. The default is 0.
User card limit	Sets the number of contactless/contact smart cards that can be associated to each user name.

Users/Cards View



By selecting **Users/Cards** from the **View** list, a list of users and their corresponding proximity card numbers can be added and registered to the SecurePrint Data Store. Importing users prevents users from having to physically register their card on a vPad device.

Components



The Components screen is where you access UniPrint component properties. All components have debugging properties, while some components have additional properties beyond debugging.

Debugging capability is implemented on all UniPrint component servers to provide additional information for troubleshooting.

Four logging levels are available: **None**, **Low**, **Medium** and **High**. To change the debug level of a component, do one of the following:

- Click to select the component, click **Set Level** and then click the desired log level.
- Right-click a component and then click the desired log level.

Most log files are created in \\Program Files\UniPrint Suite\Log Files and can be viewed by clicking on **Open Log File(s)**.

To change component settings, click to select a component and then click **Properties** or right-click a component and then click **Properties**.

Different components reside on different UniPrint component servers. All components are described below and are listed by their order of appearance on the Management Console.

UniPrint Printer Driver

This component resides on the UniPrint Bridge and on the UniPrint Application Server. If enabled, a log file UP_Driver_%timestamp%.log is created in the user's temp\Low directory, for example, C:\Users\DMorgan\AppData\Local\Temp\Low. Only the Log Level can be edited.

SecurePrint Server

This component resides on the UniPrint Bridge and is responsible for managing and accepting requests for vPad devices and virtual print queues.

If enabled, a log file, UPSPSvr_%timestamp%.log is created. This information can be used to troubleshoot connection issues between the vPad devices and the virtual print queues.

PrintPAL Server

This component resides on the UniPrint Bridge and is responsible for mapping printers to user sessions based on a combination of network administrator-defined settings and user preferences.

If enabled, a log file, UPPPSvr_%timestamp%.log is created. This information can be used to troubleshoot mapping issues with PrintPAL.

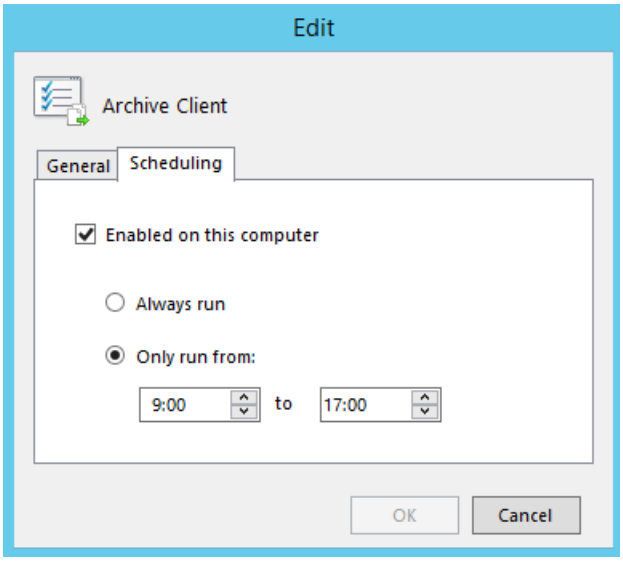
UniPrint Session Application

This component resides on the UniPrint Application Server. Only the Log Level can be edited.

If enabled, a log file UPSession-%userid%-SID2_%timestamp%.log is created in the user's temp directory. From the user's session, the log file UPSession-%userid%-SID2_%timestamp%.log can be viewed at C:\Users\%UserID%\AppData\Local\Temp.

Archive Client

This component resides on the component where print jobs are captured for archiving. If print jobs from the UniPrint queues are to be archived, then the Archive Client should reside on the same server as the UniPrint Application Server. If print jobs from Gateway printer queues are to be archived, then the Archive Client should reside on the same server as the UniPrint Print Server. This component is responsible for capturing and routing PDF print jobs to the Archive Server. The archiving can be turned on or off and archiving can be scheduled to occur only during a specified time of day. The log level can also be changed.

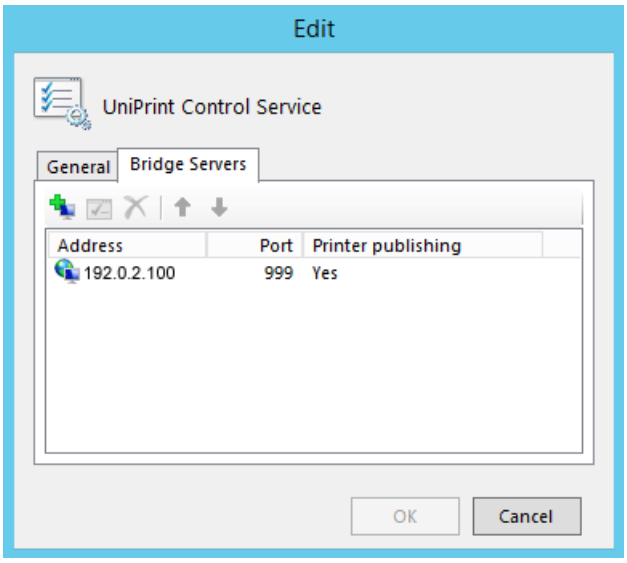


If enabled, a log file, UPArchClientSvc_%timestamp%.log is created and can be used to troubleshoot print job archiving issues.

UniPrint Control Service

This component resides on all UniPrint component servers and maintains information exchange connections with UniPrint routing servers and controls execution of UniPrint plug-ins and on-demand processors. You can edit the

Port, Log Level and add, edit or delete a Bridge connection. The default port is 998.



If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot connectivity issues with the UniPrint Bridge.

Active Directory console processor

This component resides on the Bridge and is responsible for processing Active Directory requests from the Management Console. Only the log level can be edited.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created and can be used to troubleshoot directory requests from the Management Console to Active Directory.

Active Directory Processor

This component resides on the UniPrint Bridge and is responsible for Active Directory queries. Only the log level can be edited.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot queries to Active Directory.

Alternate Server Plugin

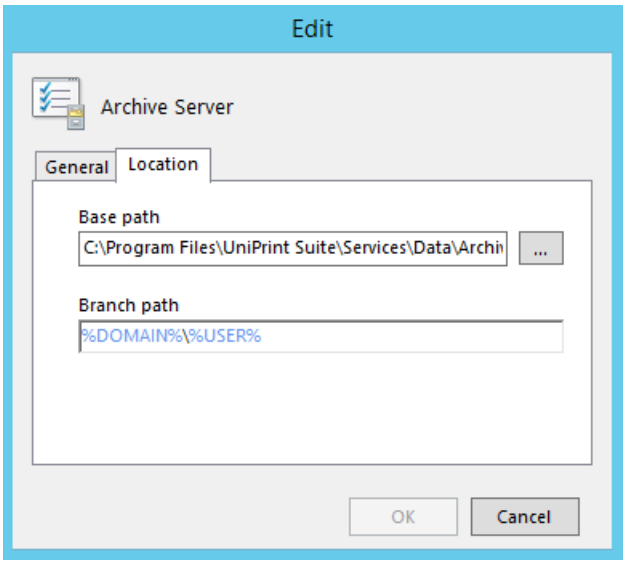
This component resides on the UniPrint Bridge and is responsible for managing alternate server nodes for traffic rerouting. Only the log level can be edited.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot HA routing issues at failover.

Archive Server

This component resides on the server machine where print jobs are to be archived. It can also reside on any other UniPrint component, for example, the UniPrint Bridge, as long as it points to a different network accessible

location. The Archive Server is responsible for managing and routing a copy of all print jobs received from the Archive Client. The Log Level and the archive location can be set.



If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot connection and routing issues between the Archive Client and the archive location.

Bridge server info processor

This component resides on the UniPrint Bridge and when queried provides information on the Bridge such as cluster information if the Bridge is a member of a cluster or printer mapping information for PrintPAL.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot what information is passed between the Bridge and the inquiring component.

Connected node management plug-in

This component resides on the UniPrint Bridge and manages the presence of active UniPrint nodes and services node-related requests. Only the Port and Log Level settings can be edited. The default port is 25469.

If enabled, a log file UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot active nodes and services.

Document conversion processor

This component resides on the Bridge and enables document conversion between various formats and PDF. The port and the log level can be edited. The default port is 10701.

If enabled, two log files are created, UPDocCnvrtSvr_%timestamp%.log and UPDocCnvrt_%timestamp%.log and can be used to troubleshoot issues with print job conversion to PDF format for Email2Print.

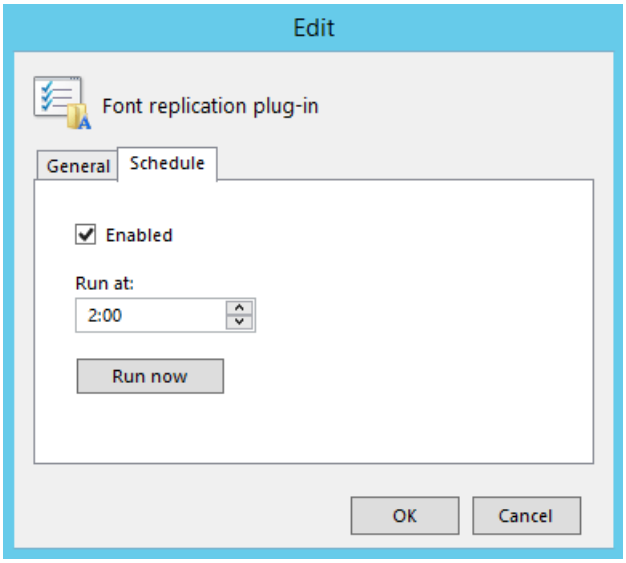
Email2Print Server

This component resides on the UniPrint Bridge and is responsible for processing and printing incoming e-mail attachments to the designated printer. Only the log level can be edited.

If enabled, a log file UPE2PSvr_%timestamp%.log is created. This information can be used to troubleshoot Email2Print issues.

Font replication plug-in

This component resides on the UniPrint Print Server and manages font availability by requesting fonts from UniPrint Application Server(s) once daily at the scheduled time. Font replication eliminates the occasional need to embed fonts when printing through UniPrint. The Log Level and replication schedule can be set.



If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot issues regarding font replication on the UniPrint Print Server.

Font request processor

This component resides on the UniPrint Application Server. It marshals and completes font list and font requests from remote print servers. Only the Log Level can be edited.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot issues regarding font replication.

FTP print job processor

This component resides on the UniPrint Bridge and enables printing directly to FTP-enabled printers. Only the Log Level can be edited.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot Lexmark/HP FTP printer connections.

License manager plug-in

This component resides on the UniPrint Bridge and is responsible for active license administration and distribution. Only the Port and Log Level can be edited. The default port is 25467.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot license management issues.

License request processor

This component resides on the UniPrint Bridge and marshals license requests from remote servers and relays these requests to the license manager plug-in. Only the Log Level can be edited.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot license requests from remote Application Servers.

Management console connector

This component resides on all three UniPrint Infinity components and marshals Management Console requests across all UniPrint Infinity nodes. Only the log level can be edited.

If enabled, a log file, UPCtlSvc_%timestamp%.log, is created and can be used to troubleshoot issues with Management Console requests between the different UniPrint Infinity nodes.

Management console HTTP server to enable web-based administration

This component resides on the Bridge. and enables the web-based administration for Print Route. Only the log level can be edited.

If enabled, a log file, UPCtrlSvc_%timestamp%.log, is created and can be used troubleshoot issues with Print Route

Node identification plug-in

This component resides on all UniPrint component servers and serves to identify itself on the UniPrint node network. Only the Log Level can be edited.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot issues regarding local node identification.

Node request processor

This component resides on the UniPrint Bridge and marshals connected node requests from remote servers and relays these requests to the Node identification plug-in. Only the Log Level can be edited.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot issues regarding remote node requests.

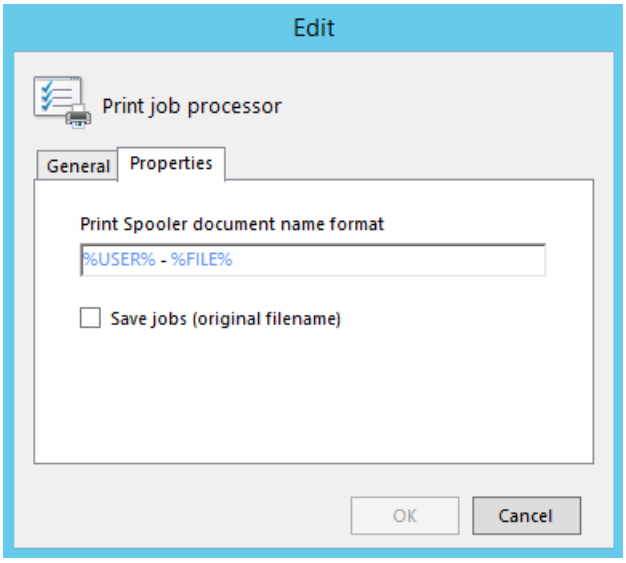
Print Job storage processor

This component resides on the UniPrint Bridge and accepts print jobs designated for SecurePrint and/or the UniPrint VPQ. It is also responsible for submitting print job information to the SecurePrint Data Store.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot issues regarding printing to SecurePrint and the UniPrint VPQ.

Print job processor

This component resides on the UniPrint Print Server and accepts print jobs from servers and relays information to the UniPrint rendering engine. It is also responsible for monitoring and reporting print job status back to the originating server. The Log Level and Port number can be edited and print jobs can be set to be saved with a specified naming convention. The default port is 10206 and naming convention is %USER%-%FILE% which are placeholders for user name and file name. The naming convention refers to the print job name displayed in the print queue. If the **Save jobs** option is enabled, print jobs are saved on the UniPrint Print Server in %ProgramFiles%\UniPrint Suite\Services\Data\PrintJob.



If enabled, a log file, UPPrintJobSvr_%timestamp%.log is created. This information can be used to troubleshoot issues regarding print job monitoring and reporting.

Printer change monitor

This component resides on the Bridge and Print Server and monitors local print server printers and relays changes to subscribers. The port and log level can be edited. The default port number is 32112.

If enabled, a log file, UPCtlSvc_%timestamp%.log, is created. This information can be used to troubleshoot issues regarding local printer information not being relayed to other UniPrint components and services.

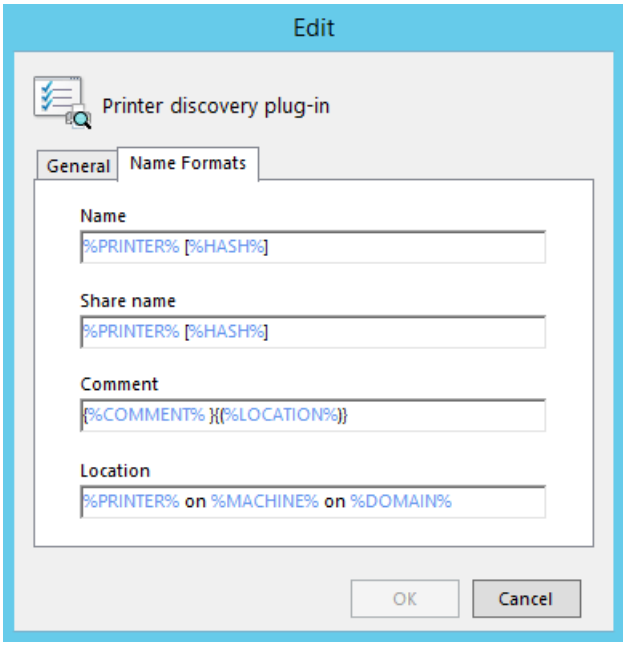
Printer creation processor

This component resides on the UniPrint Bridge and handles the creation and maintenance of UniPrint Gateway queues from remote print servers. Only the Log Level can be edited.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot printer replication from a connecting UniPrint Print Server.

Printer discovery plug-in

This component resides on both the UniPrint Bridge and the UniPrint Print Server and monitors local print server printers and relays changes to the UniPrint Bridge. The Log Level can be edited to provide greater detail and publishing naming formats can be rearranged as desired.



If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot issues regarding print server printer monitoring.

Printer discovery plug-in (Bridge)

This component resides on the UniPrint Bridge and monitors local Bridge printers and relays changes to client sessions. Only the Log Level can be edited.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot issues regarding the VPQ.

Printer lookup optimization plug-in

This component resides on both the UniPrint Bridge and the UniPrint Print Server and is responsible for internal list generation and maintenance of available printers. It optimizes performance since the list can be used to look up printers before enumerating the Windows spooler.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot printer unavailability issues.

Printer settings synchronization processor

This component resides on the UniPrint Bridge and marshals printer setting changes across UniPrint Bridges in a UniPrint environment. Only the log level can be edited.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot Gateway printer property issues in an HA environment.

PrintPAL Server Relay

This component resides on the UniPrint Bridge and marshals PrintPAL Client requests from remote servers and relays these to the PrintPAL Server for user printer data acquisition. Only the Log Level can be edited.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot mapping issues with PrintPAL.

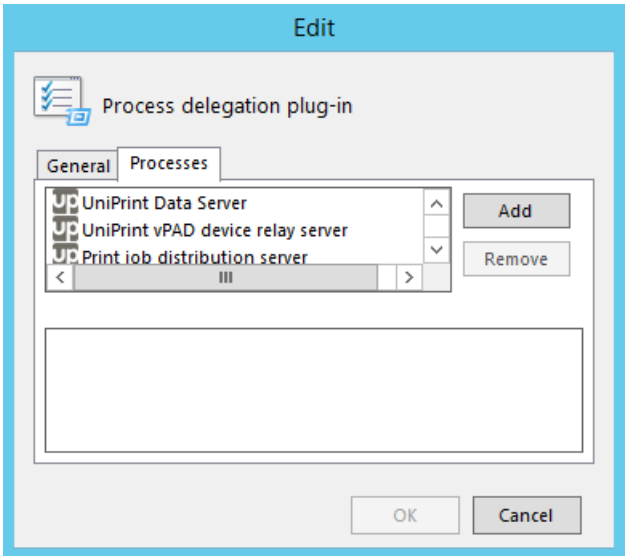
PrintPAL Settings Syncing Plugin

This component resides on the UniPrint Bridge and is responsible for syncing PrintPAL setting with an external database. Only the log level can be edited.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot PrintPAL issues in an HA environment.

Process delegation plug-in

This component resides on all UniPrint component servers and starts and monitors UniPrint-related processes. The Log Level can be edited and processes can be added or removed.



If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot issues regarding UniPrint-related processes.

Profile discovery plug-in

This component resides on the UniPrint Print Server and is responsible for monitoring print profile activity and synchronizing profile changes with the UniPrint Data Store. This component is only used in environments with UniPrint vPad devices. Only the log level can be changed.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot issues with detecting profiles on the UniPrint Print Server.

Quorum synchronization plug-in

This component resides on both the UniPrint Bridge and the UniPrint Print Server and maintains synchronization of cluster quorum files with locally stored UniPrint configuration data.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information is only relevant for failover clusters and can be used to troubleshoot issues regarding quorum path availability.

Remote Console query processor

This component resides on all UniPrint component servers and enables the UniPrint Management Console to process commands initiated from remote system nodes. Only the Log Level can be edited.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot issues regarding command processing from remote UniPrint component servers.

SecurePrint Job processor

This component resides on the UniPrint Print Server and accepts print jobs from the SecurePrint & VPQ Servers and relays information to the UniPrint rendering engine. Only the Log Level can be edited.

If enabled, a log file, UPPrintJobSvr _%timestamp%.log is created. This information can be used to troubleshoot issues regarding SecurePrint printing.

UniPrint Bridge 64-bit layer plug-in

This component resides on the UniPrint Bridge and provides compatibility for 32-bit to 64-bit printing. Only the Log Level can be edited.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot issues regarding the Windows-On-Windows support layer.

UniPrint Bridge service discovery plug-in

This component resides on the UniPrint Bridge and is responsible for responding to UniPrint Bridge IP discovery requests. Only the Log Level can be edited.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot issues regarding Bridge IP requests from remote servers.

UniPrint compressed Printstream relay server

This component resides on the UniPrint Print Server and is responsible for relaying compressed print data traffic from the print server to vPads. The Log Level and Port number can be edited. The default port number is 10212.

If enabled, a log file, UPPrintStreamRelaySvr_%timestamp%.log is created. This information can be used to troubleshoot issues regarding print stream compression between the print server and the vPad device.

UniPrint Data Server

This component resides on the UniPrint Bridge and manages information exchange between SecurePrint & VPQ subsystem and the vPad devices. It also acts as a SecurePrint database access layer. The Log Level and Port number can be edited. The default port number is 10209.

If enabled, a log file, UPDataAgent_%timestamp%.log is created. The information can be used to troubleshoot connection issues between SecurePrint/VPQ and vPad devices.

UniPrint driver install plug-in

This component resides on the UniPrint Bridge and the UniPrint Application Server and installs the UniPrint printer driver. Only the Log Level can be edited.

If enabled, a log file, UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot issues regarding driver and port installation and removal.

UniPrint vPAD device relay server

This component resides on the UniPrint Print Server and relays information to and from vPad devices. It also acts as a conduit to the SecurePrint database layer. The Log Level and Port number can be edited. The default port number is 10208.

If enabled, a log file, UPDeviceRelaySvr_%timestamp%.log is created. This information can be used to troubleshoot connection issues between the Print Server and the associated vPad device.

UniPrint printer install plug-in

This component resides on both the UniPrint Bridge and the UniPrint Application Server and installs the UniPrint printer, port and port monitor. Only the Log Level can be edited.

If enabled, a log file UPCtlSvc_%timestamp%.log is created. This information can be used to troubleshoot issues regarding the UniPrint printer installation.

UniPrint SecurePrint & VPQ server

This component resides on the UniPrint Bridge and manages print job information and data between the SecurePrint & VPQ subsystem and the vPad devices. It also acts as a SecurePrint database access layer. Only the port number and log level can be edited. The default port is 10207.

If enabled, a log file, UPDeviceSvr_%timestamp%.log is created. This information can be used to troubleshoot connection and information transfer issues between the SecurePrint Server and the vPad devices.

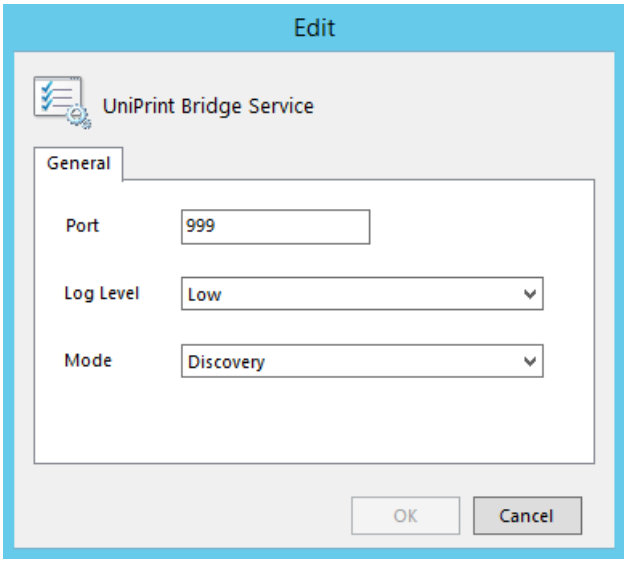
UniPrint IPP Service

This component resides on the UniPrint Print Server and enables AirPrint printing for published UniPrint Gateway printers. Only the port number and the log level can be edited. The default port is 10502.

If enabled, a log file, UPIPPSvc_5timestamp%.log is created. This information can be used to troubleshoot any issues with publishing Gateway printers as Apple-compatible printers.

UniPrint Bridge Service

This component resides on the UniPrint Bridge and acts as an information router between UniPrint nodes. It also authenticates and manages connections between UniPrint Control Services. The Port, Log Level and Mode can be changed. The default port is 999.



If enabled, a log file UPSplSvc_%timestamp%.log is created. This information can be used to troubleshoot issues regarding incoming connections from other UniPrint nodes.

Discovery mode

Allows any UniPrint Print Server or UniPrint Application Server to become a subscriber of the UniPrint domain.

Locked Down

When enabled, new subscribers are not allowed to join the UniPrint domain.

Other Log Files

Other log files exist for components and services that are not listed in the Components screen can be used to troubleshoot various issues in UniPrint Infinity.

UPStatSvc_%timestamp%.log
This log file can be used for troubleshooting issues with the Statistics Server.

UPStatClientSvc_%timestamp% .log
This log file can be used for troubleshooting issues with the Statistics client and capturing print statistics.

UPPrintPALCacheSvr_%timestamp%.log
This log file can be used for troubleshooting issues with AD caching in PrintPAL.

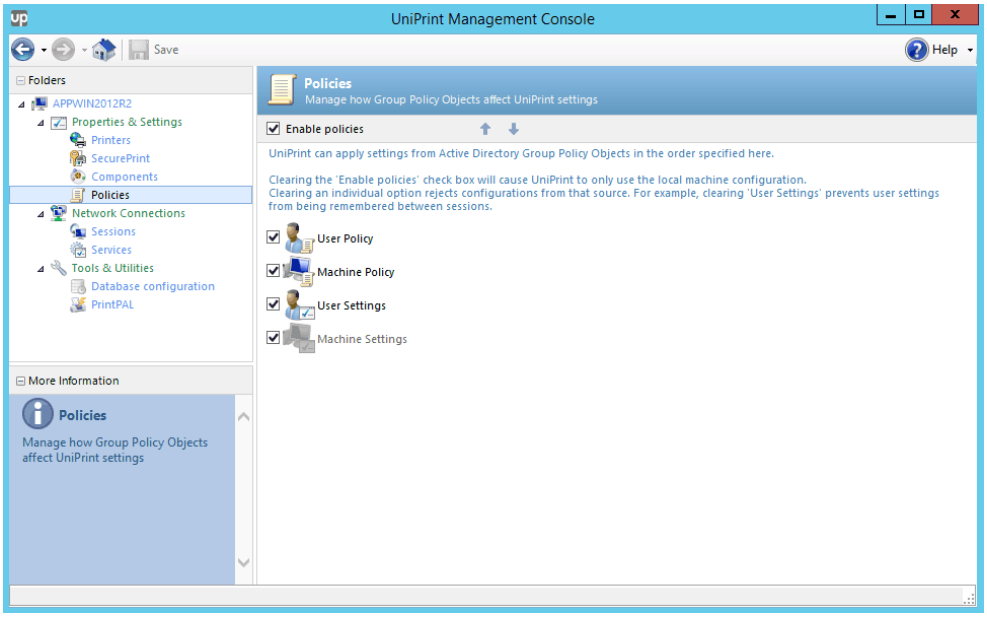
UPImprivataSvr_%timestamp%.log
This log file can be used for troubleshooting issues with Imprivata authentication integration.

UPAUXSvc_%timestamp%.log
This log file can be used for troubleshooting issues with the Auxiliary server and SecurePrint with regards to printing to Apple-compatible printers.

UPDeviceHTTPSSvr_%timestamp%.log
This log file can be used for troubleshooting issues with various VPQ Connectors for print job release.

UPChromeSvc_%timestamp%.log
This log file can be used for troubleshooting issues with the UniPrint Mobile Server.

Policies



Administrators can configure how UniPrint applies configuration settings from alternate sources. Alternate sources include: Active Directory group policy and saved user preferences.

Selecting the **Enable policies** option instructs UniPrint to apply settings in the order of precedence set in this list. Configuration sources at the top of the list have the highest priority. To disable a source, clear the check box beside it in the list.

Clearing the **Enable policies** option forces UniPrint to apply settings based solely on the ones set from the UniPrint Management Console. This is useful when troubleshooting a configuration issue.

User policy When selected, settings configured for specific users or user groups through Active Directory group policy will be applied. This policy is only applicable to the UniPrint Application Server. (*Default is Selected*)

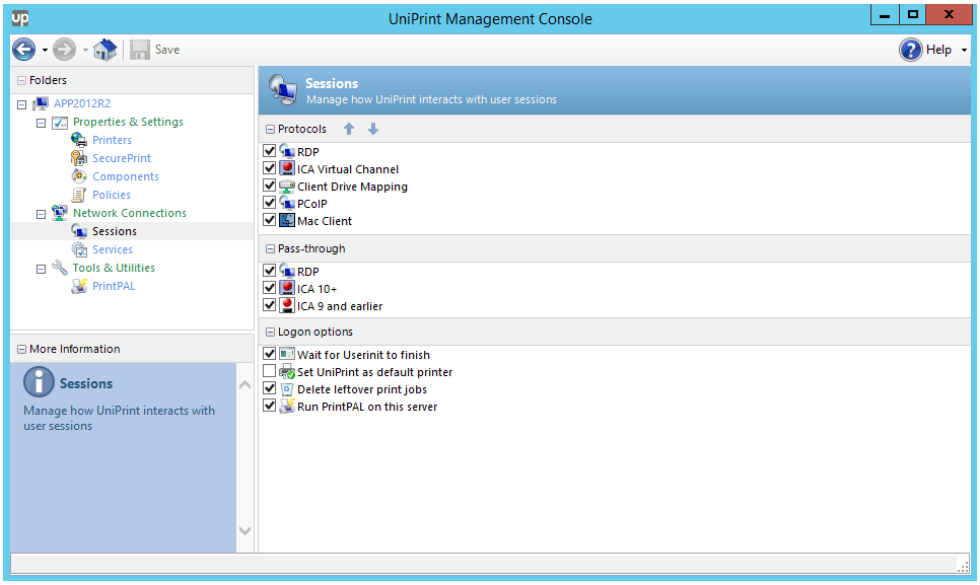
Machine policy When selected, settings configured for specific UniPrint components through Active Directory group policy will be applied. (*Default is Selected*)

User settings When selected, certain settings configured by users will be persistent across multiple ICA/RDP sessions. These settings include: Orientation, Page Size, Resolution, Paper Source and Double sided printing. They may, however, be overridden by a group policy listed higher in the processing order. This policy is only applicable to the UniPrint Application Server. (*Default is Not Selected*)

Machine settings Machine settings are default settings configured from the UniPrint Management Console and cannot be disabled. These settings always have the lowest priority. To enforce machine settings, clear **Enable policies**. (*Default is Selected and cannot be disabled.*)

Network Connections

Sessions (UniPrint Application Server only)



Protocols UniPrint supports three virtual channel protocols: RDP, PCoIP and ICA. Based on the connecting client's protocol, UniPrint creates a private, protocol-specific virtual channel between the application server and the client device for transferring rendered print jobs. Available options include:

Protocol	Comment
RDP	Does not require Citrix to be installed on the Application Server.
ICA Virtual Channel	Does not require client drive mapping to be enabled on the Citrix server.
Client Drive Mapping	Requires client drive mapping to be enabled on the Citrix server and is compatible with both Windows and non-Windows clients.

Protocol	Comment
PCoIP	Supports PCoIP for Teradici and VMware Horizon View 5.2 or later in VDI deployments. UniPrint Client 5.3 or later must be installed on the endpoint device for PCoIP to work.
Mac Client	Allows a Macintosh machine to access an Application Server.

To change the order UniPrint uses when automatically detecting the transfer protocol, click the protocol name and then click the arrow buttons to move the selected protocol up or down the list. Only the first detected transfer protocol is used. *(Default is RDP, ICA Virtual Channel, Client Drive Mapping, PCoIP, Mac Client)*

Pass-through

Selecting this option allows UniPrint to treat this Application Server as a pass-through client, routing print jobs printed from another Application Server that has UniPrint Application Server installed. As a pass-through client, UniPrint Infinity spools print jobs through chained ICA/RDP sessions where users connect from one ICA/RDP session to another by launching a second ICA/RDP session within their original session. Pass-through printing allows UniPrint Infinity to send print jobs seamlessly through multiple ICA/RDP sessions back to the first client endpoint in the chain. *(Default is Not Selected)*

Logon options

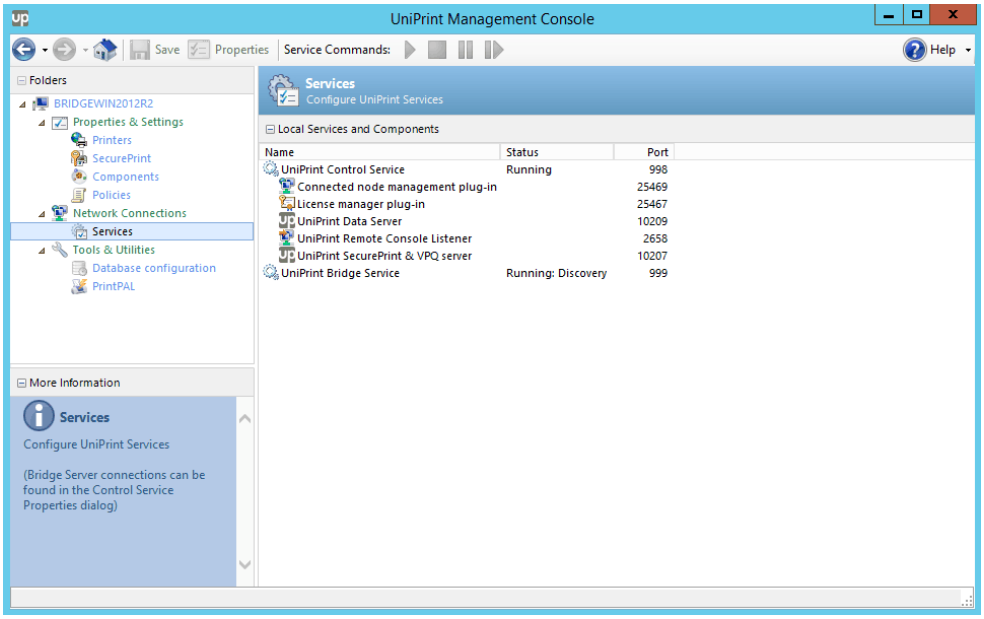
Wait for Userinit to finish
If enabled, UniPrint will wait for the Userinit Logon Application to finish before launching UniPrint UPSession. (*Default is Selected*)

Set UniPrint as default printer
When this option is selected, all users who have access to the UniPrint printer will have it set as their default printer in their sessions. *(Default is Selected)*

Delete leftover print jobs
Deletes any leftover print jobs from disconnected sessions when the same user logs back on to the Application Server. *(Default is Not Selected*)

Run PrintPAL on this server
Instructs UPSession to run PrintPAL and map printers when a session is started. *(Default is Not Selected)*

Services



UniPrint-related services can be stopped, paused and restarted. The properties of these services can also be edited by clicking the service to select it and then clicking **Properties**.

UniPrint Control Service

This service resides on all UniPrint component servers and maintains information exchange connections with UniPrint routing servers and controls execution of UniPrint plug-ins and on-demand processors. The Port and Log Level can be edited. Bridge connections can be added, edited or deleted. The default port is 998.

Connected node management plug-in

This service resides on the UniPrint Bridge and manages the presence of active UniPrint nodes and services node-related requests. Only the Port and Log Level settings can be edited. The default port is 25469.

Document conversion processor

This service resides on the UnIprint Bridge and enables document conversion between various formats and PDF. The port and log level can be edited. The default port is 10701.

License manager plug-in

This service resides on the UniPrint Bridge and is responsible for active license administration and distribution. Only the Port and Log Level can be edited. The default port is 25467.

Print job processor

This service resides on the UniPrint Print Server and accepts print jobs from servers and relays information to the UniPrint rendering engine. It is also responsible for monitoring and reporting print job status back to the originating server. The Log Level and Port number can be edited and print

jobs can be set to be saved with a specified naming convention. The default port is 10206 and naming convention is %USER%-%FILE% which are placeholders for user name and file name. The naming convention refers to the print job name displayed in the print queue. If the **Save jobs** option is enabled, print jobs are saved on the UniPrint Print Server in %ProgramFiles%\UniPrint Suite\Services\Data\PrintJob.

Printer change monitor

This service resides on the UniPrint Bridge and UniPrint Print Server and monitors local print server printers and relays changes to subscribers. The log level and port number can be edited. The default port is 32112.

UniPrint compressed Printstream relay server

This services resides on the UniPrint Print Server and is responsible for relaying compressed print data traffic from the Print Server to vPads. The Log Level and Port number can be edited. The default port number is 10212.

UniPrint Data Server

This service resides on the UniPrint Bridge and manages information exchange between SecurePrint and VPQ subsystem and the vPad devices. It also acts as a SecurePrint database access layer. The Log Level and Port can be edited. The default port is 10209.

UniPrint vPad device relay server

This service resides on the UniPrint Print Server and relays information to and from vPad devices. It also acts as a conduit to the SecurePrint database layer. The Log Level and Port can be edited. The default port is 10208.

UniPrint Remote Console Listener

This service resides on all UniPrint component servers and accepts console commands from remote servers. Only the Port can be edited. The default port is 2658.

UniPrint SecurePrint & VPQ server

This service resides on the UniPrint Bridge and manages print job information and data between the SecurePrint & VPQ subsystem and the vPad devices. It also acts as a SecurePrint database access layer. Only the port number and log level can be edited. The default port is 10207.

UniPrint Bridge Service

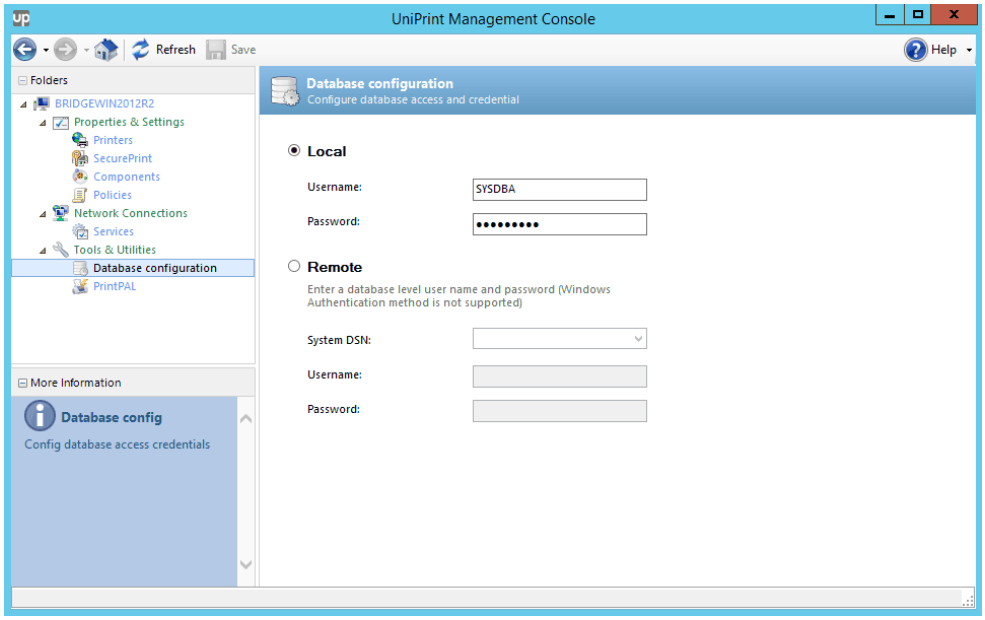
This service resides on the UniPrint Bridge and acts as an information router between UniPrint nodes. It also authenticates and manages connections between UniPrint Control Services. The Port, Log Level and Mode can be changed. The default port is 999.

UniPrint IPP Service

This service resides on the UniPrint Print Server and enables AirPrint printing module for printers published through UniPrint Gateway. The port and log level can be edited. The default port is 10502.

Tools & Utilities

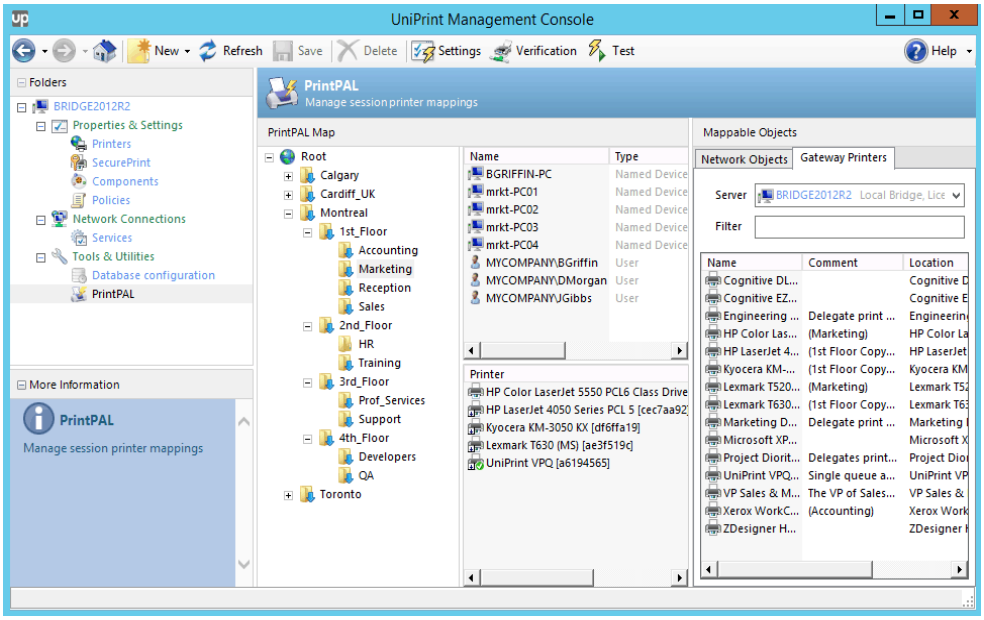
Database Configuration



UniPrint Infinity relies on a Firebird database for features such as SecurePrint and print job statistics, for example. Unless you plan on deploying UniPrint in a high availability configuration, the Firebird database should be more than sufficient and doesn't require additional configuration.

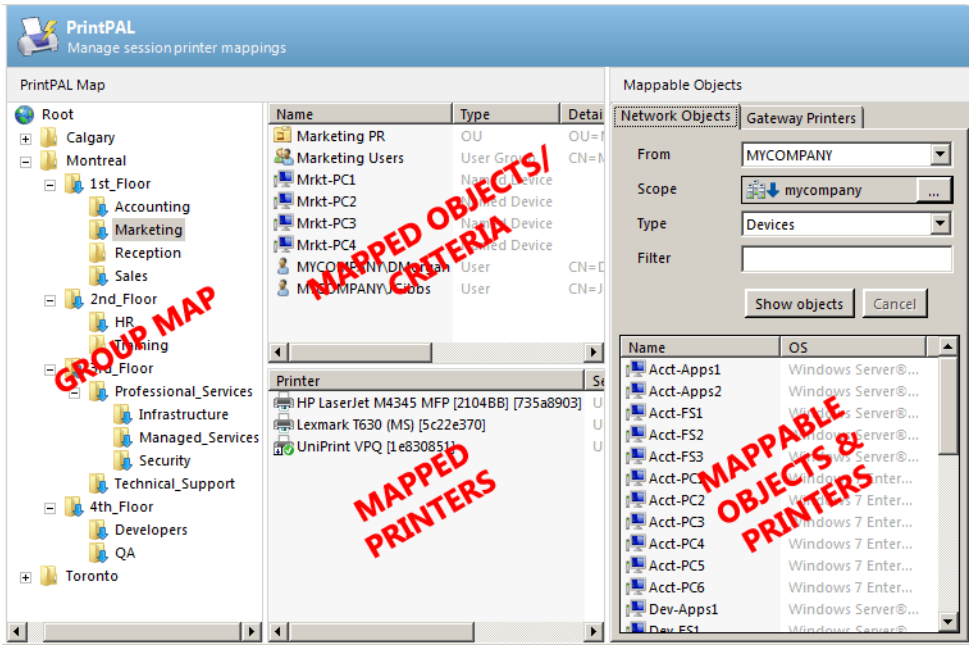
However for high availability, we recommend using a remote, centralized database such as Microsoft SQL Server. After installing a new database, a script will need to be run which creates UniPrint tables. For more information on the high availability setup, see the UniPrint Infinity High Availability Setup Guide.

PrintPAL



PrintPAL is a printer to user session mapping utility that is installed on the UniPrint Bridge. It provides a simple user interface that enables administrators to control or restrict which Gateway printers are initially added to a user's or group of users' sessions. Administrators first create groups of client devices, OUs, user groups and users and then map them to specific printers.

PrintPAL is comprised of four panes. The panes on the left side represents the PrintPAL map and the pane on the right side represents mappable objects which consists of network objects and Gateway printers.



Group Map

This pane represents your device group mapping in tree form. Use this pane to create parent and child groups to which devices and printers are mapped and then grouped. Groups can be organized geographically, departmentally and are typically dependant on your network topology and corporate organization.

Mapped Objects/ Criteria

This pane displays the devices (for example, servers, PCs, thin clients and PDAs), users, user groups and organizational units assigned to the selected group. If **Match all criteria types** is enabled for the group, then this pane contains all of the required criteria types to be matched before printers are mapped to a session. The screen shot above contains a list of objects assigned to the Marketing group on the 1st Floor in Montreal.

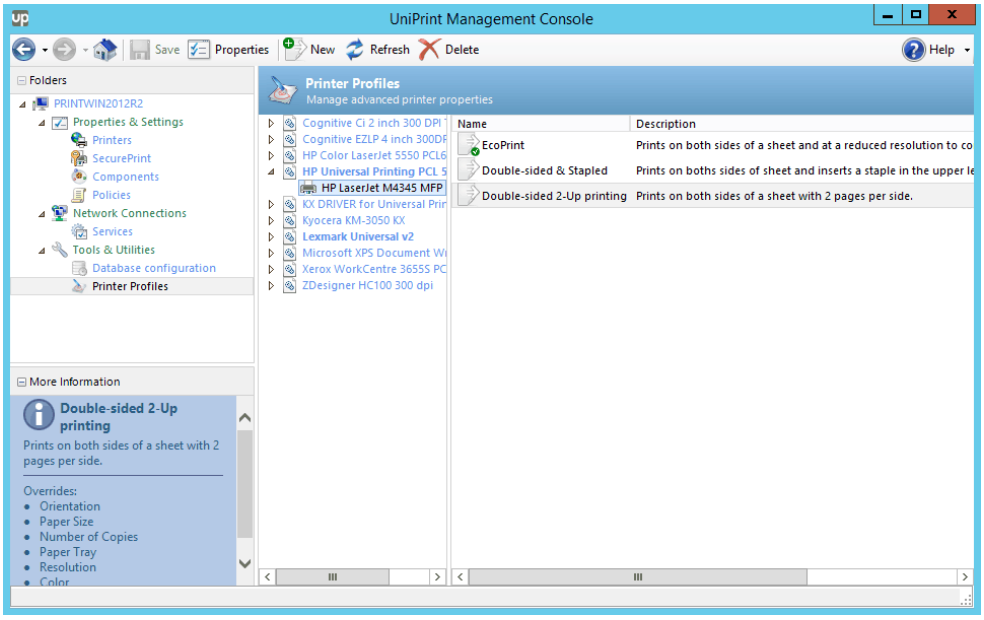
Mapped Printers

This pane displays the printers added to the devices listed in the **Mapped Objects** pane. During a client session, a user will initially have access to any of the Gateway printers listed in this pane.

Mappable Objects & Printers

This pane lists all the objects that are from the domain specified in PrintPAL **Settings** and is divided into two tabs. The **Network Objects** tab lists all of the devices, users, user groups and OUs. The **Gateway Printers** tab lists all of the mappable printers. Objects can be dragged into the **Mapped Objects** pane and printers can be dragged to the **Mapped Printers** pane. This assigns these objects and printers to the selected group.

Printer Profiles (UniPrint Print Server Only)



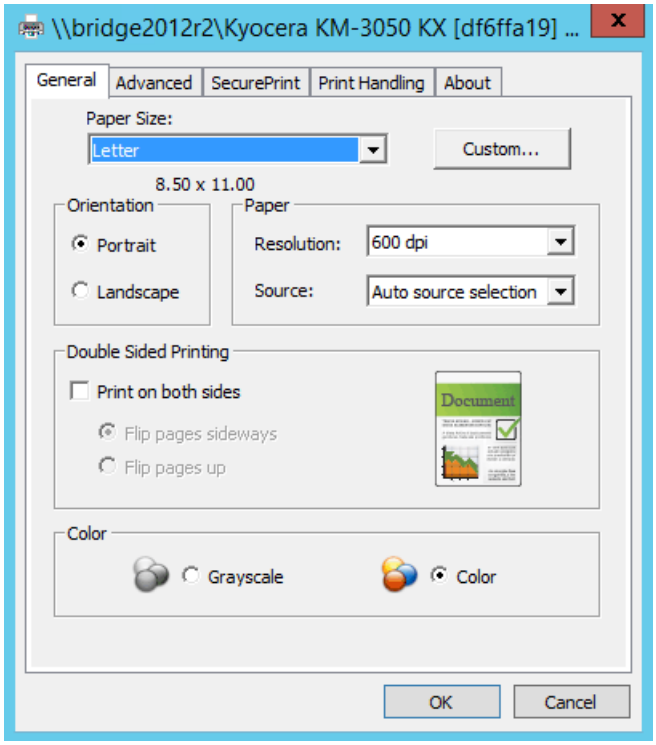
Printer Profiles resides on the UniPrint Print Server and can be used to enable advanced printer properties such as stapling, hole punching, binding, etc., that some printers support since it directly accesses the native printer driver.

Advanced printer properties can also be grouped together making it easier for users to print their document exactly as intended with only one mouse click.

Gateway Printer Properties Interface

You can change Gateway Printer Properties on a job-by-job basis. These properties affect how the PDF file is created and processed when you click **Print**. In some cases, printer properties (for example, orientation) may be automatically changed by the application from which you are printing. The property set in the application will take precedence over Gateway Printer Properties.

General Tab



Paper Size

This option sets the paper size for this print job. The various paper sizes and forms listed match those supported by the printer. The UniPrint printer supports standard sizes and any custom forms defined on the Application Server.

Orientation

The orientation of a document can be set to either Portrait or Landscape. Portrait orients the document vertically while Landscape orients the document horizontally. Applications that set this parameter internally take precedence. Microsoft Word, for example, sets the Layout Orientation internally.

Paper

Resolution The resolution for a document can be set to 72, 150, 300, 600, 1200 or 2400 dpi. This option mainly affects image resolution, but text precision can also be improved by increasing this value. The designated printer must be capable of printing at the desired resolution setting.

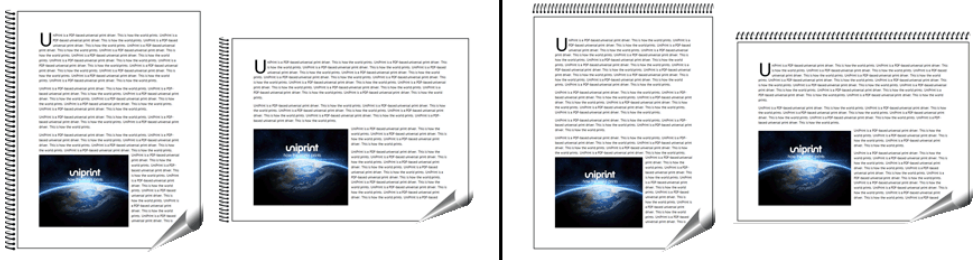
Source This option sets the paper tray source. The available options are Auto Select, Manual Feed, Envelope Feed and up to six tray selections.

Double Sided Printing

This option sets the double-sided printing functionality when **Print on both sides** is selected. The designated printer must have duplexing capabilities.

Flip pages up This refers to tablet style documents.

Flip pages sideways This refers to booklet style documents.



Flip pages sideways

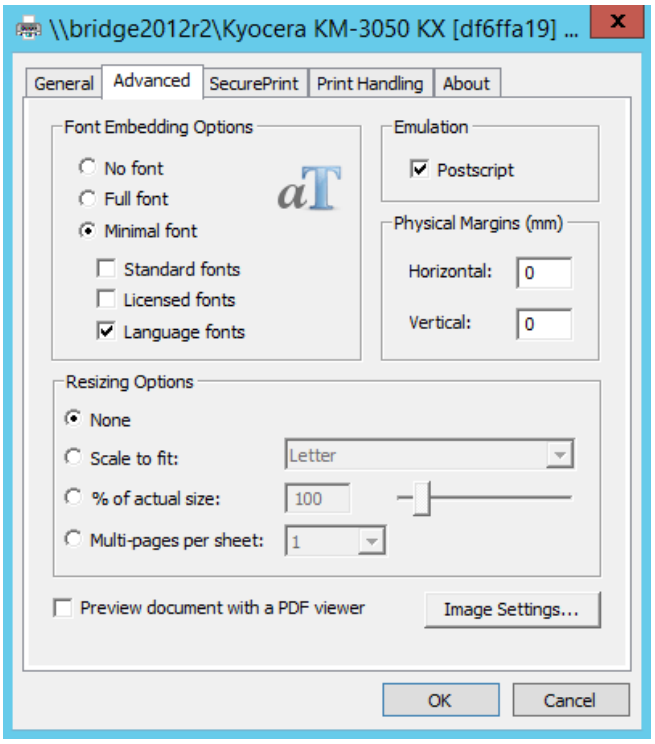
Flip pages up

Color

Grayscale Selecting this option instructs UniPrint to render the print job in grayscale. It will convert color images into shades of black and white that best suit the original image.

Color This option is best for printers that utilize the R(Red), G(Green), B(Blue) color space and is also recommended for documents that will be displayed online or viewed on a computer monitor.

Advanced Tab



Font Embedding Options

Fonts are software and subject to license restrictions. Standard fonts are commonly found within operating systems and applications, and are legally transferable. Licensed fonts are, however, generally specialized fonts that are purchased and subject to license terms and conditions.

No font Selecting this option instructs UniPrint not to include any fonts in the output PDF file. This results in much smaller files being transferred and depends on the Print Server having the appropriate fonts installed for proper rendering.

Full font Selecting this option instructs UniPrint to include all True Type and Type1 (PostScript) fonts used by the source document in the output PDF file. This results in larger files but ensures a consistent look to the document on any platform.

Minimal font Selecting this option instructs UniPrint to embed only portions of the font file that are used by the source document.

Standard fonts
If selected, UniPrint will embed the Arial and Times New Roman font files. These fonts are not embedded by default since they are provided with Adobe Reader.

Licensed fonts
If selected, UniPrint will embed licensed fonts that are installed on the Application Server. However, the fonts may not be embedded if the font license agreement prohibits embedding.

Language fonts
If selected, UniPrint will convert characters that are not in Western European or US character sets (such as Eastern European and Far Eastern characters). This conversion tends to increase the file size.

Emulation

PostScript Enabling this option emulates the UniPrint printer driver as a PostScript printer to the application. This is particularly useful when printing documents with vector graphics such as WordArt objects or semi-transparent backgrounds from Microsoft Office.

Physical margins (mm)

Most printers have a minimum physical margin below which they cannot generate any output. Each printer's mechanical design dictates the size of this printable area and the size of the margins. Applications use this value to prevent users from drawing outside the printable area.

Horizontal Specifies the margin from the left and right edge of the paper.

Vertical Specifies the margin from the top and bottom edge of the paper.

Resizing Options

Although PDF files can be created as large as 38 100 000 cm in either direction, most desktop printers cannot print large documents. To print oversized documents you can select one of the appropriate options.

Scale to fit Expands or shrinks the original document to fit on a specified paper size. This option changes the size of the created PDF.

% of actual size Expands or shrinks the document by a specified percentage. If the percentage is increased too much, the document will only print the upper left area of the document.

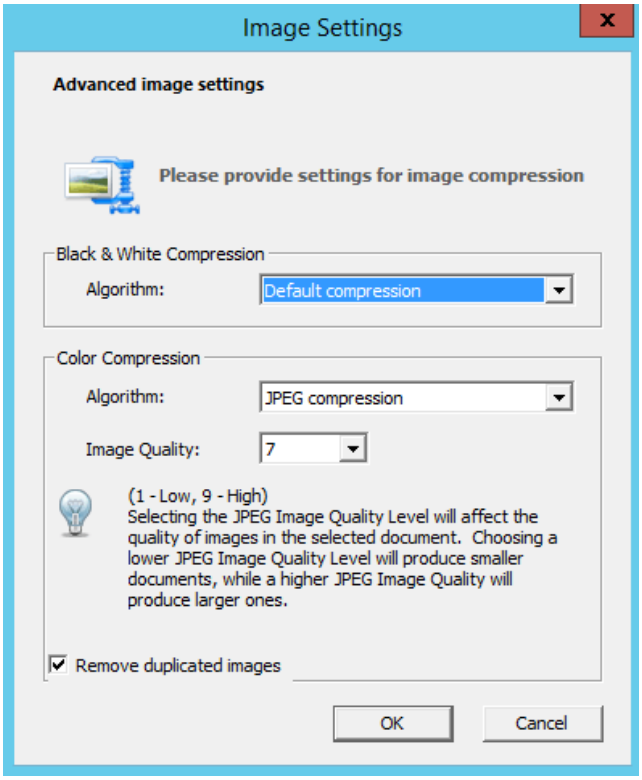
Multi-pages per sheet

Enables N-up printing, whereby multiple pages are printed on a single sheet of paper. Multi-pages per sheet is done intelligently to maximize legibility with the number of pages per sheet selected and the original orientation of the document. This option changes the document size so that it can be saved as a PDF.

Preview document with a PDF viewer

If enabled, Adobe Reader will be invoked prior to printing for preview purposes. Adobe Reader must first be installed on the UniPrint Application Server.

Image Settings Button



The following algorithms set the desired image compression for black and white and color images which results in a smaller file size.

Black & White Compression

Default compression

This algorithm makes use of color palettes to reduce the overall size of all images including black and white images and it works well as long as the number of colors does not exceed 256.

CCITT Fax Group 4

The CCITT Fax Group 4 algorithm is recommended to reduce the size of black and white images. Image quality is not affected by this type of compression but file sizes can be greatly reduced.

Color Compression

Default compression

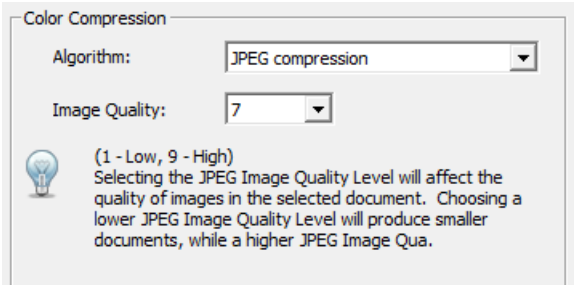
For color images, **Default compression** makes use of color palettes to reduce the overall size of all images. This algorithm works well as long as the number of colors does not exceed 256.

256 color compression

The 256 color compression algorithm calculates the most used 256 colors in an image and replaces all other color pixels by their closest match. This compression algorithm works very well with most applications but is relatively slow on large images with a greater number of colors.

JPEG compression

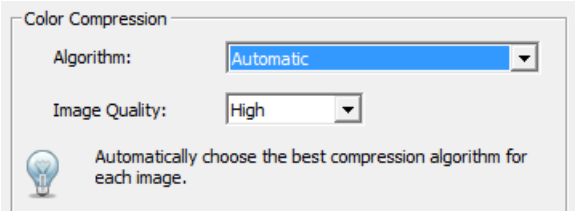
This compression algorithm produces excellent results for real life true color images with a small distortion of the source image. Since it removes image data and may reduce image quality, compressing images that have already been compressed using JPEG compression will lead to additional loss of information. It is, therefore, not recommended for graphics other than photographs.



When JPEG compression is selected, the **JPEG Image Quality Level** selection box appears, allowing you to choose from level 1 to 9. Level 1 produces lower quality images with very large compression ratio, whereas level 9 produces higher quality images with medium compression ratios. The default level is 7, which produces image quality suitable for most situations.

Automatic

With this compression algorithm, each image is analyzed separately to determine the best suited compression algorithm. The best suited compression algorithm is then applied to the individual image.

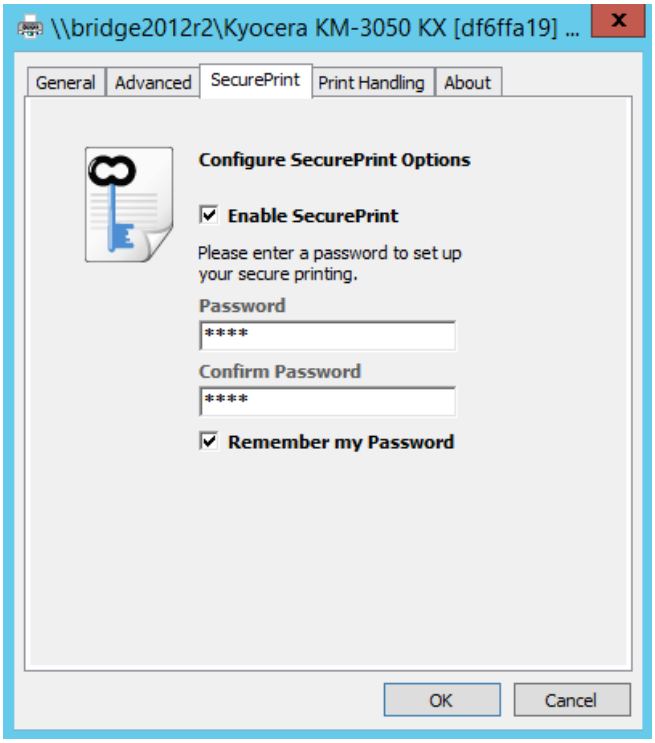


When Automatic compression is selected, the Image quality selection box appears, allowing you to choose between Maximum, High, Medium, Low and Minimum. The default level is *Maximum*, which will provide optimal results.

Remove duplicated images

If enabled, UniPrint Infinity, will remove any duplicate images from the generated PDF file. This setting is enabled in the registry on the UniPrint Application Server.

SecurePrint Tab

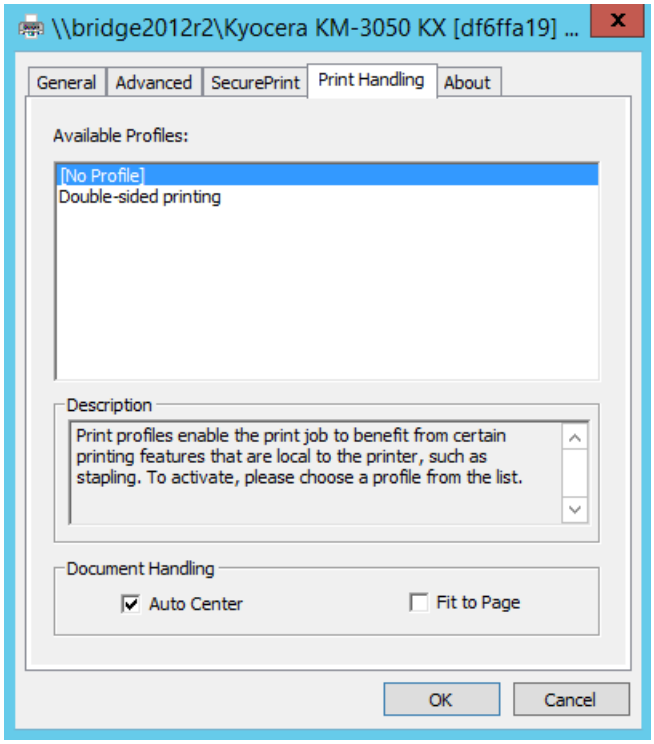


This feature allows users to set a password, which is then entered at a vPad device to release their print jobs. To set a password for SecurePrint, the

Enable SecurePrint option must be selected. To set a password on a job-by-job basis, ensure that **Remember my password** is disabled.

NOTE: This feature only applies to Gateway and UniPrint VPQ printers and will be disabled for the UniPrint printer, UniPrint (Email PDF), UniPrint (Save PDF), and any delegate queues.

Print Handling Tab



NOTE: This tab and its features are only applicable to Gateway printers and will not appear for the UniPrint, UniPrint (Email PDF), UniPrint (Save PDF), UniPrint VPQ, and delegate print queues.

Available profiles

By selecting a print profile, documents can be printed using a combination of advanced printer properties set in each profile. A description of each profile is given below.

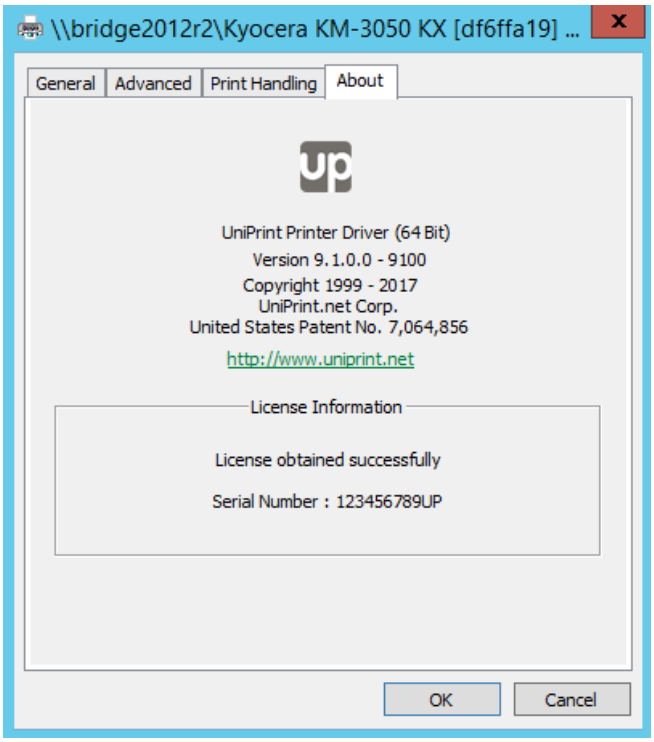
At least one printer profile must be created on the UniPrint Print Server before this area will be enabled.

Document Handling

Auto Center When set, document content will be both horizontally and vertically centered on a page.

Fit To Page When set, the document content is shrunk to fit the paper size selected in the **General** tab. This option does not affect the PDF file size.

About Tab



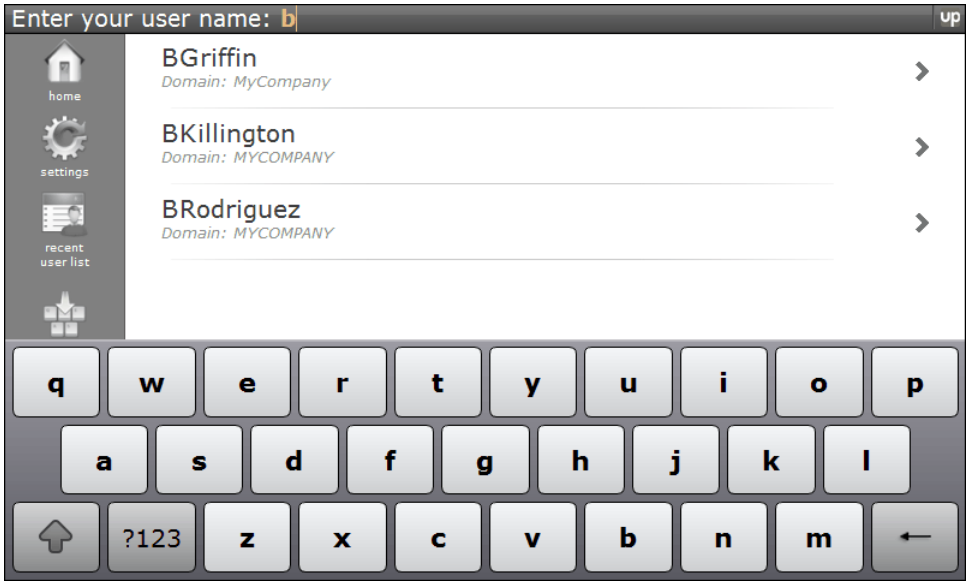
The **About** tab contains information about the UniPrint printer driver version and license information. If the license information box is blank or states "Unable to obtain a valid license", a watermark banner will be printed across each page.

vPad Console Interface

The vPad console is a user interface that is used to retrieve print jobs sent to the virtual print queue (VPQ) or to a Gateway printer queue. After a password is set in printer properties and the document is sent to print, the user simply goes to the vPad device. To release their print job, the user either enters or taps their user name and then enters their password.

The console itself does not store the print job. It simply notifies the UniPrint Bridge to release the print job.

Console Home



In the console Home page, the user initially searches for their user name after clicking **Print**. Depending on which Home page is set as the default, the user can either do a search by entering their user name with the keyboard or they can search a list of recently searched users.

In order to appear in the Recently Searched Users List, the user must have searched for their user name at least once. If this is first time using the vPad, then their user name will not appear on this list. A limited number of user

names maintained on the Recently Searched Users List can also be set by tapping **Settings**, **Advanced** and then tapping the **Recent User List** tab.

To return to the home page, tap **Home**

.

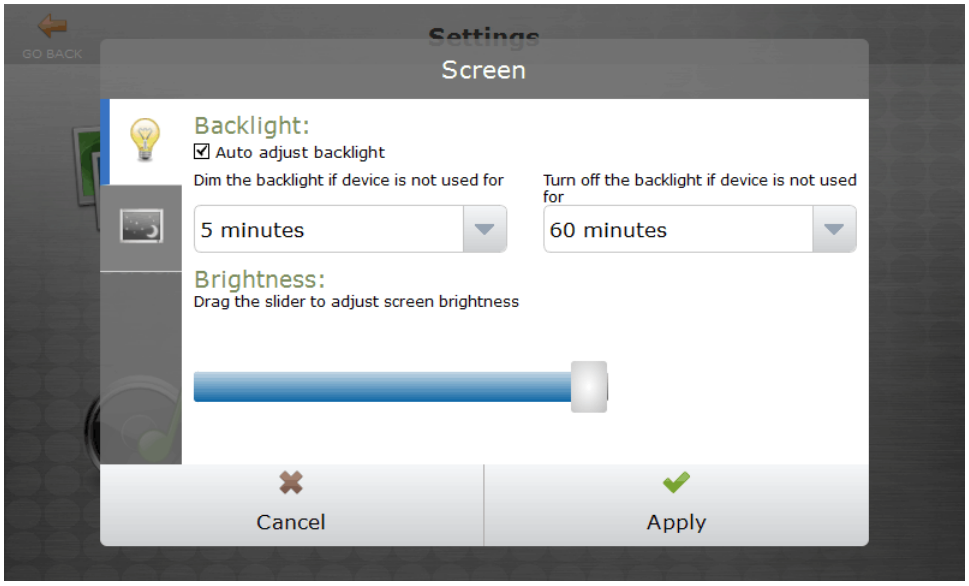
Settings

Use **Settings**

to configure the vPad device itself not the SecurePrint print jobs. Configuration settings such as screen backlighting, default home page, user interface language, sound and vPad device information are accessible through this screen.

To return to the home page, tap the orange back arrow at the top.

Screen



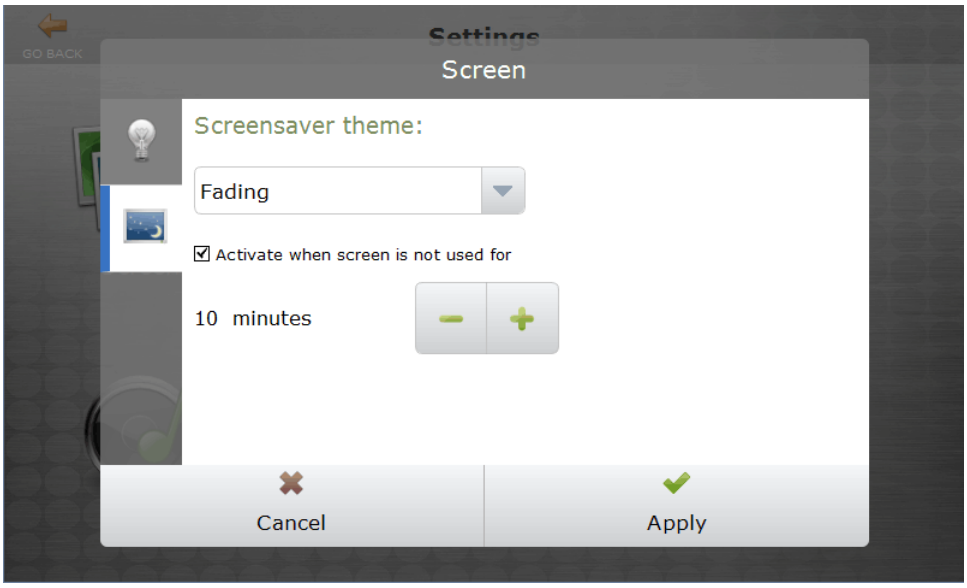
The Screen configuration settings are used to adjust backlighting and display brightness. You can also set the screen idle time to dim the display and also to turn off the display.

Backlight

Auto adjust backlight
If selected, the screen will dim at the time selected under **Dim the backlight if device not used for** and turn off the backlight at the time selected under **Turn off the backlight if device not used for**. This features helps to conserve energy and prevents image persistence on the vPad display. The default time to dim is 5 minutes and the default time to turn off is 60 minutes.

Brightness

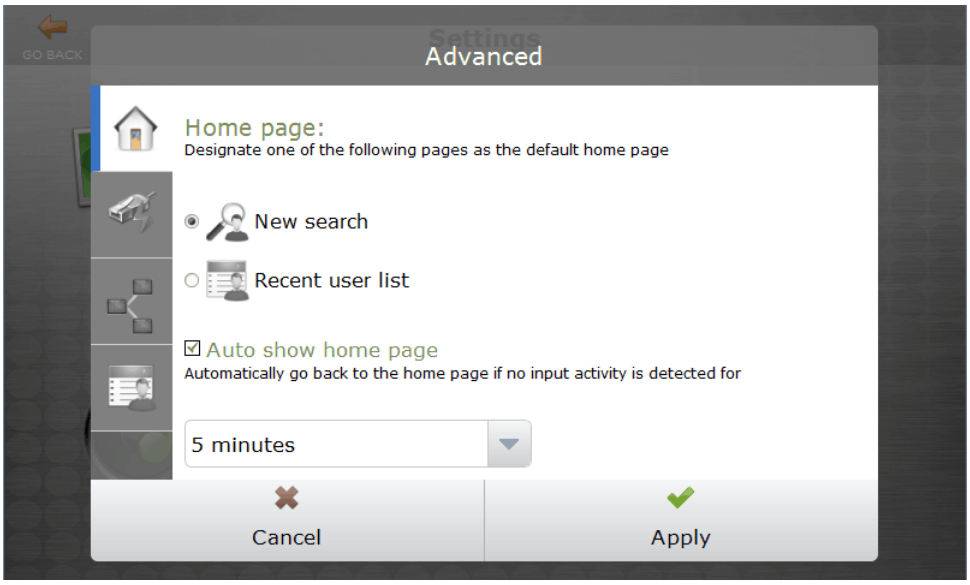
Use the slider to adjust the brightness of the backlight from 0% on the far left to 100% on the far right. The default brightness is set to 100%



Screensaver theme

The screensaver can either be set to Fading or Blank. Setting a screensaver on the vPad could help avoid image persistence. The screen idle time can also be set. By default the screensaver is disabled.

Advanced



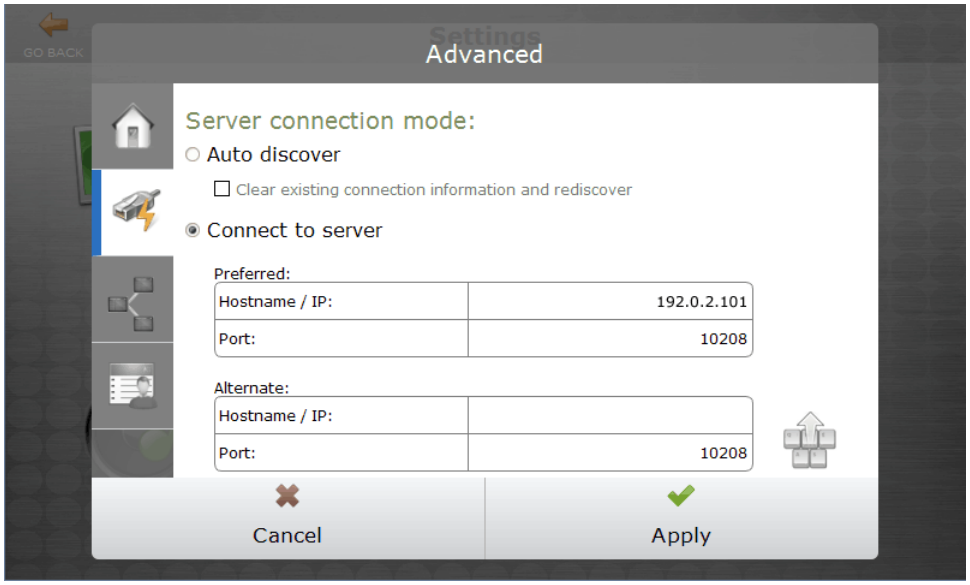
Through the Advanced settings, you can change the default home page, by clicking the HOME tab, change the IP address of the associated printer server by clicking the CONNECTION tab, configure ethernet connection by clicking the NETWORK tab, and adjust the number users maintained on the recently searched user list by clicking the NOTEPAD tab.

Home page

In the HOME tab, the default home page can be changed from **New search** where the user has to key in their user ID to **Recent user list** where the user can scroll through a list of users. By default the home page is set to **New search**.

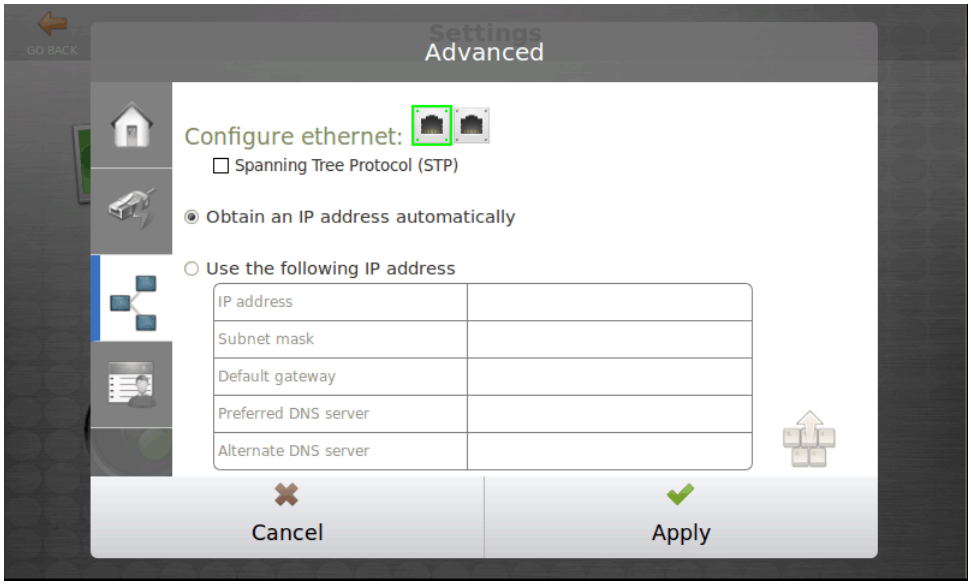
Auto show home page

If enabled, the screen will refresh to the home page selected above at the selected screen idle time. The default screen idle time is 15 seconds.



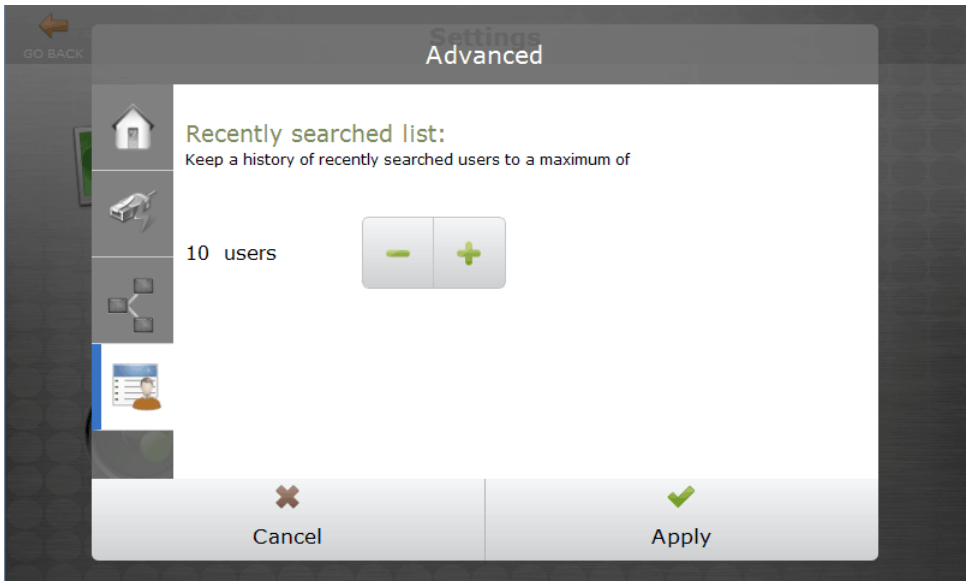
Server connection mode

The connection mode can either be set to auto-discover a UniPrint Print Server or you can enter the IP address of the UniPrint Print Server using the key pad.



Configure ethernet

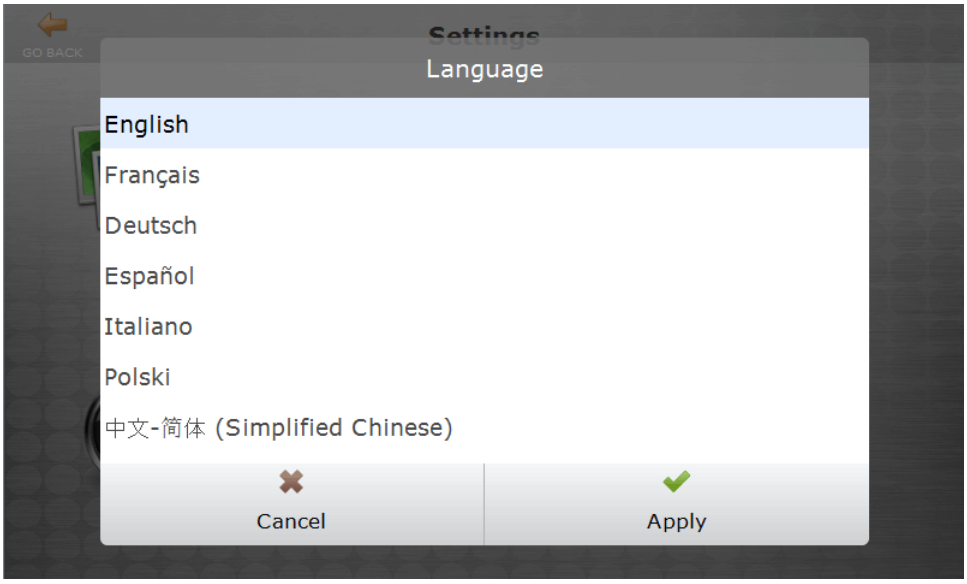
A static IP address can be assigned to the vPad device by selecting **Use the following IP address** and enter the static IP address. This feature does not apply to the SecurePrint emulator and the screen is therefore disabled on the emulator. To assign a static IP address, ensure that the vPad is connected to eth1 (the green highlighted port). The right port that is not highlighted is for bridge configurations. If it is deemed necessary that both ports be connected to the network, ensure that **Spanning Tree Protocol (STP)** has been selected to prevent bridge loops from being created. For more information, see "Assigning a Static IP Address To The vPad Pro" on page 279.



Recently searched list

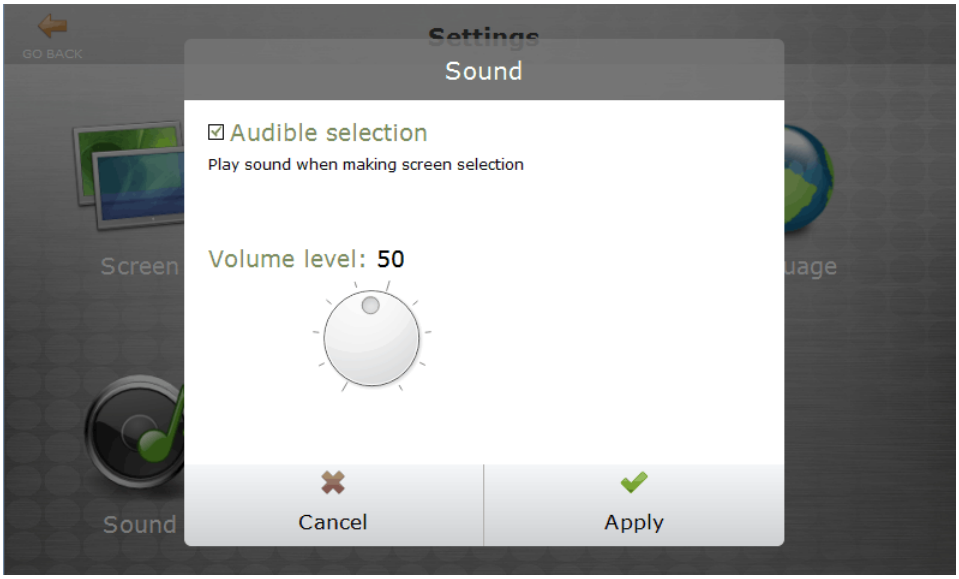
Sets the maximum number of users displayed on the recently searched list. The default number of user names is 10.

Language



English, French, German, Spanish, Italian, Polish and simplified Chinese user interface languages are now available.

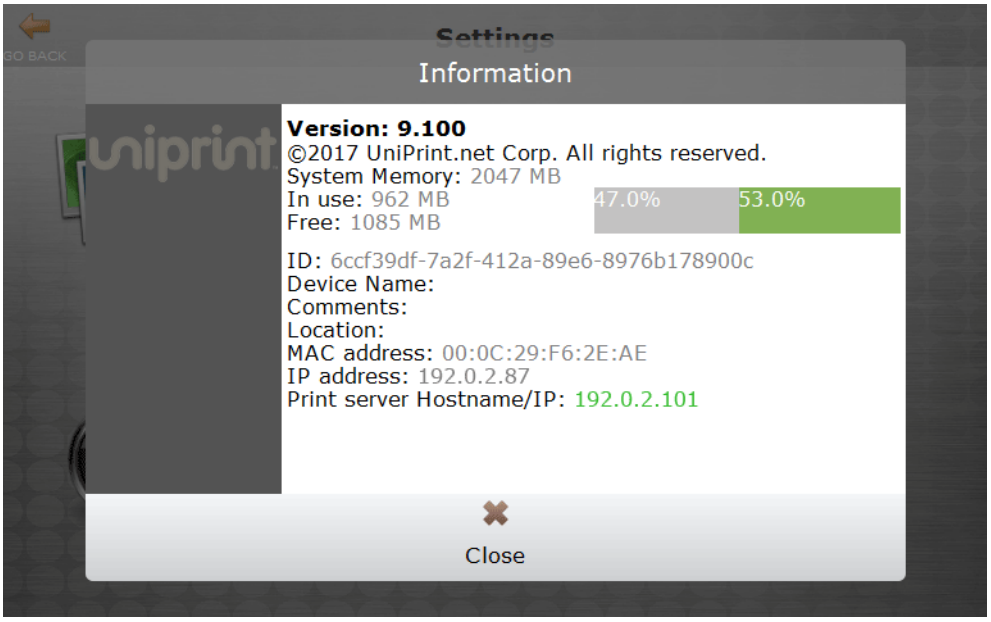
Sound



Audible selection If enabled, the vPad will emit a sound each time the screen is tapped.

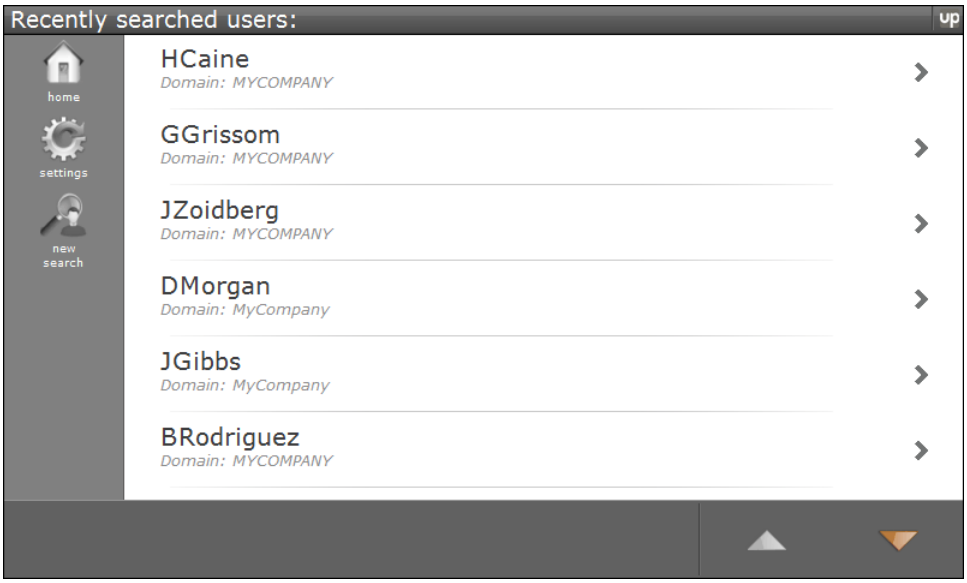
Volume level The volume level can be set from 0% (quiet) farthest counter-clockwise to 100% (loud) farthest clockwise. The default volume level is 50%.

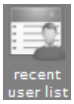
Information



This screen contains information regarding the vPad device, for example, the amount of memory left, the IP address of the device and the IP address of the UniPrint Print Server it is connected to.

Recent User List

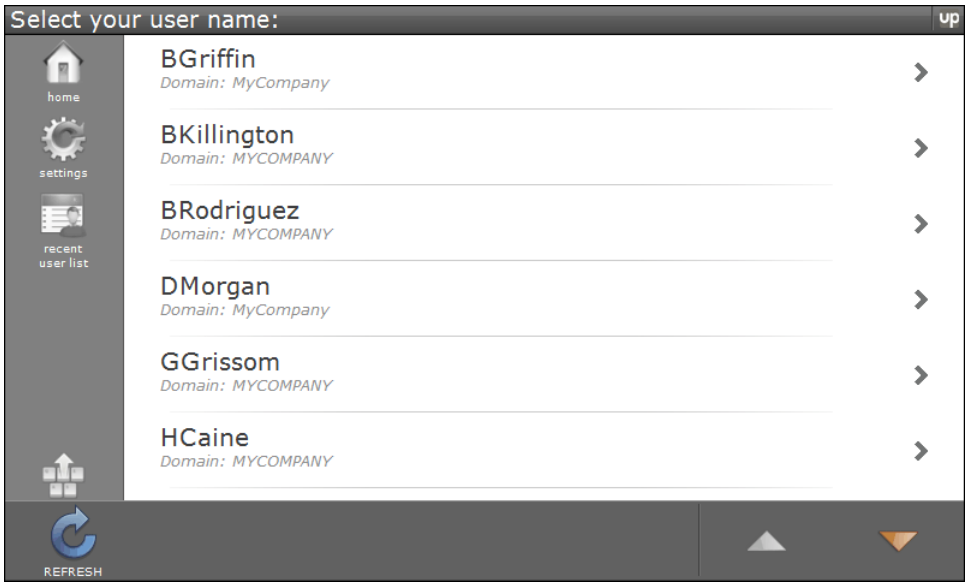


Tapping 

reveals the Recent Users List. This screen contains a list of user IDs that have been recently searched. If the user has yet to search for their user ID, then their user ID will not appear on this list and they may want to either search for their User ID or scroll through the Pending Print Jobs User list.

To access a list of print jobs initiated by a particular user, click the user name.

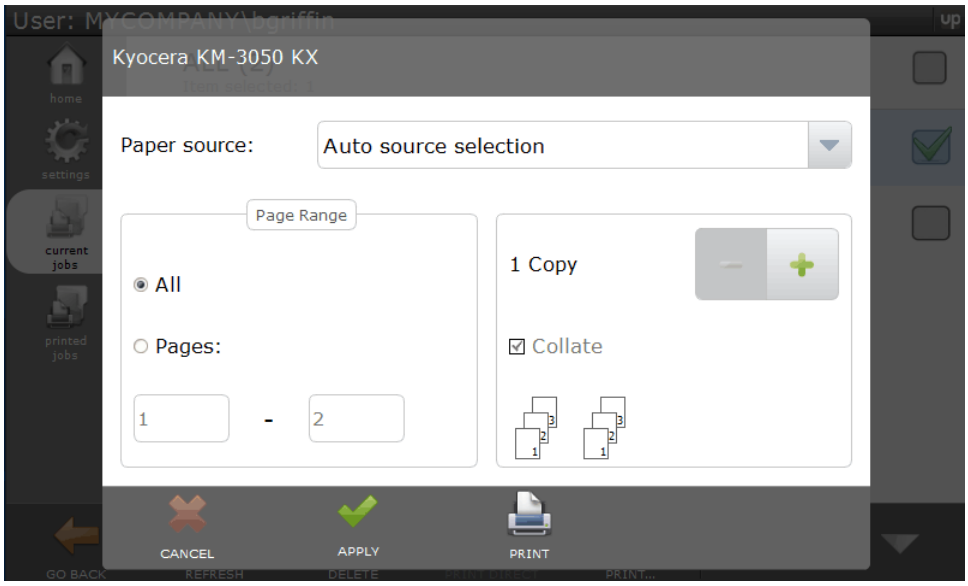
Pending Print Jobs User List



Tapping Hide Keypad reveals a list of users that have print jobs waiting to be released.

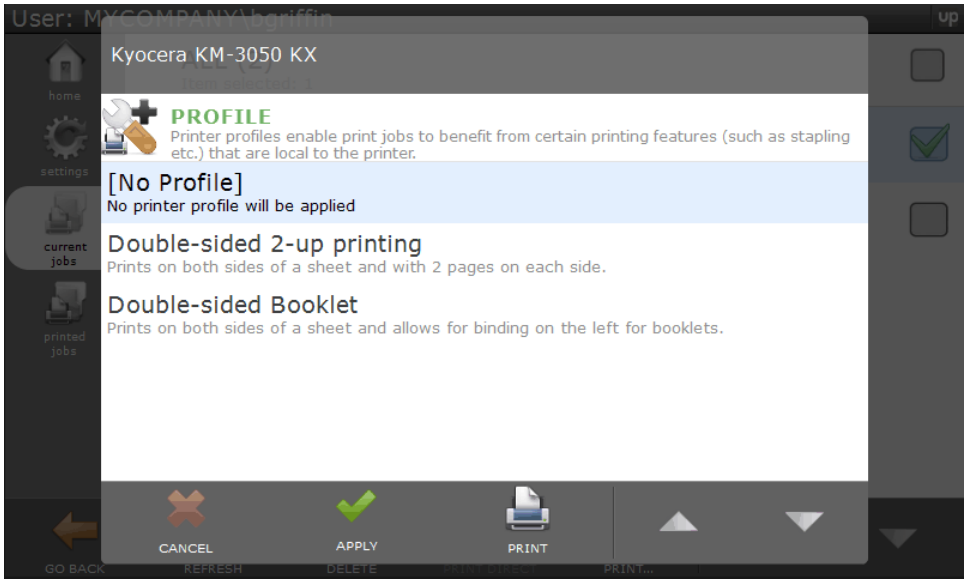
To access a list of print jobs to release, tap the user name.

Printer Settings



Before the print job is released, users have the option to change printer settings such as paper source, page range and number of copies.

Profile



If users print to the UniPrint VPQ, they are not given an option to select a printer profile before clicking **Print** in the application. At the vPad, before

the print job is released, users can select a printer profile to apply to their print job. The default is **No Profile**.

Paper Sizes

Use this table for the UP_SETTING_PAPERSIZE = **n**, when installing UniPrint Application Server from the command line.

The following is a list of paper sizes supported by UniPrint:

n	**Description**
1	Letter (8 1/2 x 11 in)
2	Letter Small (8 1/2 x 11 in)
3	Tabloid (11 x 17 in)
4	Ledger (17 x 11 in)
5	Legal (8 1/2 x 14 in)
6	Statement (5 1/2 x 8 1/2 in)
7	Executive (7 1/4 x 10 1/2 in)
8	A3 (297 x 420 mm)
9	A4 (210 x 297 mm)
10	A4 Small (210 x 297 mm)
11	A5 (148 x 210 mm)
12	B4 (JIS) (257 x 364 mm)
13	B5 (JIS) (182 x 257 mm)
14	Folio (8 1/2 x 13 in)
15	Quarto (215 x 275 mm)
16	10 x 14 in
17	11 x 17 in
18	Note (8 1/2 x 11 in)
19	Envelope #9 (3 7/8 x 8 7/8 in)
20	Envelope #10 (4 1/8 x 9 1/2 in)

n	Description
21	Envelope #11 (4 1/2 x 10 3/8 in)
22	Envelope #12 (4 3/4 x 11 in)
23	Envelope #14 (5 x 11/2 in)
24	C size sheet (17 x 22 in)
25	D size sheet (22 x 34 in)
26	E size sheet (34 x 44 in)
27	Envelope DL (110 x 220 mm)
28	Envelope C5 (162 x 229 mm)
29	Envelope C3 (324 x 458 mm)
30	Envelope C4 (229 x 324 mm)
31	Envelope C6 (114 x 162 mm)
32	Envelope C65 (114 x 229 mm)
33	Envelope B4 (250 x 352 mm)
34	Envelope B5 (176 x 250 mm)
35	Envelope B6 (176 x 125 mm)
36	Envelope Italy (110 x 230 mm)
37	Envelope Monarch (3.875 x 7.5 in)
38	6 3/4 Envelope (3 5/8 x 6 1/2 in)
39	Std Fanfold (14 7/8 x 11 in)
40	German Std Fanfold (8 1/2 x 12 in)
41	German Legal Fanfold (8 1/2 x 13 in)
42	B4 (ISO) (250 x 352 mm)
43	Japanese Postcard (100 x 148 mm)
44	9 x 11 in
45	10 x 11 in
46	15 x 11 in
47	Envelope Invite (220 x 220 mm)
50	Letter Extra (9 1/2 x 12 in)

n	Description
51	Legal Extra (9 1/2 x 15 in)
52	Tabloid Extra (11.69 x 18 in)
53	A4 Extra (9.27 x 12.69 in)
54	Letter Transverse (8 1/2 x 11 in)
55	A4 Transverse (210 x 297 mm)
56	Letter Extra Transverse (9 1/2 x 12 in)
57	SuperA/SuperA/A4 (227 x 356 mm)
58	SuperB/SuperB/A3 (305 x 487 mm)
59	Letter Plus (8.5 x 12.69 in)
60	A4 Plus (210 x 330 mm)
61	A5 Transverse (148 x 210 mm)
62	B5 (JIS) Transverse (182 x 257 mm)
63	A3 Extra (322 x 445 mm)
64	A5 Extra (174 x 235 mm)
65	B5 (ISO) Extra (201 x 276 mm)
66	A2 (420 x 594 mm)
67	A3 Transverse (297 x 420 mm)
68	A3 Extra Transverse (322 x 445 mm)
69	Japanese Double Postcard (200 x 148 mm)
70	A6 (105 x 148 mm)
71	Japanese Envelope Kaku #2 (240 x 332 mm)
72	Japanese Envelope Kaku #3 (216 x 277 mm)
73	Japanese Envelope Chou #3 (20 x 235 mm)
74	Japanese Envelope Chou #4 (90 x 205 mm)
75	Letter Rotated (11 x 8 1/2 in)
76	A3 Rotated (420 x 297 mm)
77	A4 Rotated (297 x 210 mm)
78	A5 Rotated (210 x 148 mm)

n	Description
79	B4 (JIS) Rotated (364 x 257 mm)
80	B5 (JIS) Rotated (257 x 182 mm)
81	Japanese Postcard Rotated (148 x 100 mm)
82	Double Japanese Postcard Rotated (148 x 200 mm)
83	A6 Rotated (48 x 105 mm)
84	Japanese Envelope Kaku #2 Rotated (332 x 240 mm)
85	Japanese Envelope Kaku #3 Rotated (277 x 216 mm)
86	Japanese Envelope Chou #3 Rotated (235 x 120 mm)
87	Japanese Envelope Chou #4 Rotated (205 x 90 mm)
88	B6 (JIS) (128 x 182 mm)
89	B6 (JIS) Rotated (182 x 128 mm)
90	12 x 11 in
91	Japanese Envelope You #4 (235 x 105 mm)
92	Japanese Envelope You #4 Rotated (105 x 235 mm)
93	PRC 16K (146 x 215 mm)
94	PRC 32K (97 x 151 mm)
95	PRC 32K(Big) (97 x 151 mm)
96	PRC Envelope #1 (102 x 165 mm)
97	PRC Envelope #2 (102 x 176 mm)
98	PRC Envelope #3 (125 x 176 mm)
99	PRC Envelope #4 (110 x 208 mm)
100	PRC Envelope #5 (110 x 220 mm)
101	PRC Envelope #6 (120 x 230 mm)
102	PRC Envelope #7 (160 x 230 mm)
103	PRC Envelope #8 (120 x 309 mm)
104	PRC Envelope #9 (229 x 324 mm)
105	PRC Envelope #10 (324 x 458 mm)

n	Description
106	PRC 16K Rotated (215 x 146 mm)
107	PRC 32K Rotated (97 x 151 mm)
108	PRC 32K(Big) Rotated (97 x 151 mm)
109	PRC Envelope #1 Rotated (165 x 102 mm)
110	PRC Envelope #2 Rotated (176 x 102 mm)
111	PRC Envelope #3 Rotated (176 x 125 mm)
112	PRC Envelope #4 Rotated (208 x 110 mm)
113	PRC Envelope #5 Rotated (220 x 110 mm)
114	PRC Envelope #6 Rotated (230 x 120 mm)
115	PRC Envelope #7 Rotated (230 x 160 mm)
116	PRC Envelope #8 Rotated (309 x 120 mm)
117	PRC Envelope #9 Rotated (324 x 229 mm)
118	PRC Envelope #10 Rotated (324 x 458 mm)